Release Notes
Polycom® Video Border Proxy (VBP™)
VOS Version 11.2.19

11.2.19 | October 2014 | 3725-78301-003T

Trademark Information

Polycom, Inc.
6001 America Center Drive
San Jose CA 95002
USA

Introducing the Polycom VBP System Version 11.2.19

This document describes the enhancements and fixes provided by the Polycom Video Border Proxy (VBP) VoIP Operating System (VOS), version 11.2.19. This document includes all modifications made since VBP VOS version 7.2.2

What's New in the Polycom VBP System Version 11.2.19

The Polycom VBP system version 11.2.19 is a full all platforms release that resolves customer issues found in the field.

Security - Shellshock Bash vulnerabilities;

How does this affect the VBP
This vulnerability is exposed in SSH and HTTP(s), but **ONLY** to authenticated users. That is, you must have valid credentials to log into the system in order to use the exploit. This is also true whether or not you have User Management enabled.

This release addresses the bash Shellshock related issue however, following good security practices to limit exposure to the system is advised. Securing the system on the public interface is recommended by following the below steps;

Trusted Hosts
Trusted hosts should be enabled on the **VBP-E**. When Trusted Hosts are enabled and configured correctly, no attacker would be able to gain access to the system and would therefore not be able to attack the system. It is recommended to disable HTTP, HTTPS, SSH, Telnet on the WAN side of the VBP-E, however if remote support is needed for customer assistance, enabled Trusted Hosts and make sure the GUI and CLI passwords have been secured to strong passwords.

VBP-ST - disable Subscriber side HTTP, SSH and Telnet access by entering the following User Command on the VBP-ST;

Reference the VBP configuration guide;

http://supportdocs.polycom.com/PolycomService/support/global/documents/support/setup_maintenance/products/network/VBP_Configuration_Guide_11_2_6.pdf

Page = 41

To block HTTP on the Subscriber Interface
iptables -I INPUT -i eth0+ -p tcp --dport 80 -j DROP

To block HTTPS on the Subscriber Interface- NOTE: dependent on the HTTPS alternate port configured, verify the alternate HTTPS port before applying the rule.
iptables -I INPUT -i eth0+ -p tcp --dport 8443 -j DROP

To block Telnet on the Subscriber Interface
iptables -I INPUT -i eth0+ -p tcp --dport 23 -j DROP

To block SSH on the Subscriber Interface
iptables -I INPUT -i eth0+ -p tcp --dport 22 -j DROP

Disabling HTTP, HTTPS, and SSH access on WAN or Subscriber interface. If HTTP, HTTPS, and SSH access is not allowed to the WAN/Subscriber interface then, no attacker would be able to gain access to the system.

Setting user passwords
All passwords for all accounts available on the system should be set to a secure password.

Security – An issue discovered in the field with a VBP-ST system having default passwords for user “admin” and “rouser” and allowing SSH on the WAN/Subscriber interface. With the system not secured this allowed an attacker to establish a non-shell session to tunnel traffic as a relay service out the WAN/Subscriber interface.

All VBP-E and VBP-ST systems upgraded to 11.2.19 will have SSH tunneling disable.

The “admin” and “rouser” users have also been removed from shell authorization access.

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 system 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
- Polycom RealPresence Resource Manager v7.0.0 or higher
- Polycom RealPresence Mobile 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

.

- 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 systems 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.

- 5967 – ESCVIU-45 – GUI – VBP now calculates the correct bandwidth usage even after the H323 End Point down speeds during a call setup. The following mode is still outstanding and will be fix in a later release: LAN side Gatekeeper VBP-E

- 6625 – ESCVIU-64 – H.323 – WAN-Side Gatekeeper mode does not support the usage of a DNS entry, the system must have a IP address in the field.

- 5823 – ESCVIU-51 – H.323 – LifeSize Multi-point endpoints version 4.7.0 registered to the VBP Embedded Gatekeeper dialing 2 public IP endpoints. When the first endpoint being called is a LifeSize and the second endpoint is an HDX or any H.323 endpoint, the call fails to complete to the seconds endpoint. The second call is also being sent to the first endpoint – issue – When the LifeSize endpoint registered to the Embedded gatekeeper creates a port 1720 TCP connection to the first endpoint for call control, the call completes with audio and video as expected. When the second call is placed the LifeSize endpoint re-uses the same 1720 TCP connection for the second call and causes the VBP to send the SETUP to the first endpoint. When replacing the first endpoint with a HDX or other H.323 endpoint the issue does not exist. This issue is between LifeSize endpoints only; LifeSize has been contacted about this issue and will be providing a fix to the endpoint code base.

- 7570 – H.323 – H.245 sockets in listen state – When the system receives a call and processes the H.225 Q.931 message with a CONNECT, the system assigns the H.245 port to the called and calling system. If the called system hangs up before creating the TCP connection to the assigned H.245 port 14085 – 15084 the system will continue to listen for a TCP connection on this port. Over time. If the error condition continues it's possible that calls will fail to be processed by the system and a system reboot will be necessary. This error only happens when a calling system fails to create a TCP connection for H.245 negotiation. Example: When a H.323 call is initiated and hangs up immediately i.e. within 1 second it's possible the system will have a H.245 port assigned and will be in listen state.

```
# netstat -napt
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 12.48.260.10:14317    0.0.0.0:*               LISTEN      3373/mand
tcp        0      0 12.48.260.10:14445    0.0.0.0:*               LISTEN      3373/mand
```

Installation Recommendation

Platform	Upgrade Recommendation	Comment
All Platforms	All Platforms **MANDATIORY** Security update	This release will replace any Polycom version with a version string greater than 9.1.5.1. **VBP-E or VBP-ST must be upgraded**

New Features introduced in VOS 11.2.19

- None

Fixes and Enhancements in VOS 11.2.19

- EM-11611 – EM-11576 – Security - Shellshock Bash vulnerabilities – VBP-E or VBP-ST systems use GNUbash version 2.05. The following CVE's have patches applied to GNUbash 2.05;

    - CVE-2014-6277
    - CVE-2014-6278
    - CVE-2014-7186
    - CVE-2014-6271
    - CVE-2014-7169

    Note: CVE-2014-7187 is not applicable for GNUbash version 2.05

- EM-11464 – Security - **Enable SSH Tunneling** – **Item 1**: SSH tunneling is a generic option on the SSH daemon to allow a user to create an encrypted tunnel over SSH. The SSH client can be configured to forward a specified local port to an IP and port on the remote device. When the SSH tunnel is established, the user can connect to the specified local port to access the remote LAN or WAN network service. This feature is useful when supporting a customer remotely by creating a SSH tunnel to a specific host on the private trusted network. For example, this tunnel can allow the remote support person to SSH tunnel to the private LAN devices web interface for configuration assistance.

    WARNING: When enabling this feature it is advised to enable **Trusted Hosts** to only allow trusted source IP connections to manage the system. Verify all system accounts have non default passwords and are strong, containing alpha/numeric and special characters. When the feature is not required it is recommended to be disabled.

    Item 2: The admin and rouser user account has been disabled from shell authorization. Upgrading or performing a factory default will remove shell authorization for the rouser user account.

    Upgrading or performing a Factory Default of the system will force SSH tunneling to disabled. To enable the feature login to the terminal interface and edit the file /etc/config/fw_defs.conf. Change the variable - ALLOW_SSH_TCP_FWD=off - to - ALLOW_SSH_TCP_FWD=on.

    Exit the editor and save the change by entering – cfg_commit

    Restart the network by entering – config_network – **Note**: this command is service interrupting all ongoing calls will be disconnected.

    When the VBP has User Management enabled change the "admin" user account to a strong password before enabling SSH tunneling.

Example file /etc/config/fw_defs.conf
FW_ENABLE=on
ENABLE_HTTP=on
ENABLE_HTTPS=off
ENABLE_TELNET=off
ENABLE_SNMP=off
ENABLE_SSH=on
TCP_ALLOW=""
UDP_ALLOW=""
ALLOW_SSH_TCP_FWD=off

- EM-11476 – Trusted Host – Help file change - The following was added to the Help File to describe the differences for VBP-E and VBP-ST in regards to applying Trusted Hosts to the system;
    - The Trusted Hosts feature only applies as defined above to the VBP-E platform. The VBP-ST requires the Management Interface to be enabled first before restricting specific hosts or networks access on the management network to the enabled management protocols.

New Features introduced in VOS 11.2.18

- None

Fixes and Enhancements in VOS 11.2.18

- EM-10968 – Security – OpenSSL – “MiTM” Bug
    - CVE-2014-0224 – OpenSSL - OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

      The VBP uses OpenSSL version 1.0.1c which is affected by this flaw. Any service using TLS may be affected. This includes HTTPS, SSH, Access Proxy.

      ### Affected Versions

      This issue affects VBP-E or VBP-ST

VBP Version	OpenSSL version	Status
11.2.11 - HOTFIX	**0.9.8n-fips**	**Vulnerable**
11.2.12 – GA	**1.0.1c**	**Vulnerable**
11.2.16 – GA	**1.0.1c**	**Vulnerable**
11.2.17 – GA	**1.0.1c**	**Vulnerable**

      Resolution
      Applied OpenSSL patch to version 1.0.1c for CVE-2014-0224. The system will only accept a change cipher when it is expected instead of at any time. This prevents premature setting of session keys before the master secret is determined which an attacker could use as a MITM attack.

      Note: the patch is applied to OpenSSL version 1.0.1c. A security scan of the system prior to the patch does detect the issue. After the OpenSSL patch is applied to resolve CVE-2014-0224 both Qualys Guard and Nessus security scanners are no longer detecting the issue.

- EM-10665 – Security - SSH is allowing MD5 and 96-bit MAC algorithms.
    - Disabled MD5 and 96-bit MAC algorithms for SSH connections only.

- EM-10580 – ESCVIU-162 – H.323 – Polycom RMX interoperability

    - When a RMX is registered or making a call through the VBP-E system configured for Embedded Gatekeeper mode and placing call that traverses a VBP-E configured in Peering Proxy mode if the call is unanswered by the destination the RMX re-transmits the call setup message. When the VBP-E configured for Peering Proxy mode receives the call setup re-transmission the system is counting the call twice from a bandwidth perspective. When the call fails the VBP-E Peering Proxy system did not remove all the reserved bandwidth for the call. This issue is now resolved.

- EM-10730 – ESCVIU-148 – User Management – 11th auditor fails to add

    - Adding the 11th auditor user to the system failed to add correctly in the system UI with an error message. The system did add the audit user with the username and password however did not display the user to allow the administrator to disable or delete the user. The system will now allow 52 administrator and auditor users to be configured on the system with a maximum of 30 character usernames.

      Note: this fix will NOT remove address the 11th auditor user that failed to add correctly. If the system administrator added the 11th auditor user and received and error message indicating the user failed to add, the system will require support assistance via SSH or telnet to the system to remove the failed add user's data on the file system. This includes the failed add users password data.

Fixes and Enhancements in VOS 11.2.17

- EM-10684 – Security – OpenSSL – “HeartBleed” Bug

    - CVE-2014-0160 – OpenSSL - The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets. This allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

      The VBP uses OpenSSL version 1.0.1c which is affected by this flaw. Any service using TLS may be affected. This includes HTTPS, SSH, Access Proxy.

      ## Affected Versions

      All VBP-E or VBP-ST running version 11.2.11 and below are NOT vulnerable

VBP Version	OpenSSL version	Status
11.2.11 - HOTFIX	0.9.8n-fips	Not Vulnerable
11.2.12 – GA	**1.0.1c**	**Vulnerable**
11.2.16 – GA	**1.0.1c**	**Vulnerable**

      Resolution
      The vulnerability has been resolved by re-compiling OpenSSL
      with '-DOPENSSL_NO_HEARTBEATS' to disable the vulnerable function.

      This resolution method is per the following OpenSSL Security Advisory: https://www.openssl.org/news/secadv_20140407.txt

- EM-10603 – Security – NTP "monlist" Feature Denial of Service Vulnerability

    - CVE-2013-5211 – The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.

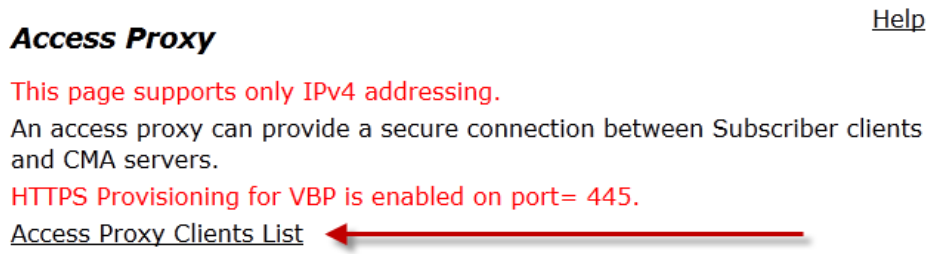
- EM-9243 – Security – PCI - ciphers using MD5 hash have been removed
- EM-9227 – ESCVIU-146 – Trusted hosted configured but ports 80 and 23 are still allowed to the VBP - When trusted hosts are enabled, ports that are not selected on the firewall are not being blocked.
- EM-9853 – ESCVIU-158 - Network - Incorrectly using IPv6 on H.323 calls - When IPv6 is not configured on the system, and if an IPv6 result is returned from the DNS SRV lookup as the best result for the domain, the system will select this result.
- 10688 – ESCVIU-159 – H.323 – Downspeed in LAN-Side Gatekeeper mode – Added support to the system to downspeed using the Notify message when the system is configured for LAN-Side Gatekeeper mode. Note: some gatekeepers do not forward the Notify message during call origination.

New Features introduced in VOS 11.2.16

- None

Fixes and Enhancements in VOS 11.2.16

- 9864 – Security – OpenSSH - PCI Compliance scans may report the following issue as a PCI compliance failure – the issue is now resolved. OpenSSH has been upgraded to version 6.1p1
    - CVE-2011-5000 - The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field.
- 10034 – ESCVIU-128 - Security – NTP - PCI Compliance scans may report the following issue as a PCI compliance failure – the issue is now resolved. NTPD version 4.2.4p4 has been back ported from NTP version 4.2.6p5 to address CVE-2009-1252. Furthermore, the vulnerable code is only reachable if ntpd is configured to use autokey, indicated by a "crypto pw <password>" in the ntpd.conf file. VBP does not use autokey configuration setting, therefore severely limiting, if not completely eliminating an occurrence of this attack method. NTPD has back-ported the fix for this issue from NTP version 4.2.6p5 to address CVE-2009-3563. Engineering has supplied a document explaining the patches applied to NTPD 4.2.4p4 to resolve these two CVE's. This document is available upon request.
    - CVE-2009-1252 - Stack-based buffer overflow in the crypto_recv function in ntp_crypto.c in ntpd in NTP before 4.2.4p7 and 4.2.5 before 4.2.5p74, when OpenSSL and autokey are enabled, allows remote attackers to execute arbitrary code via a crafted packet containing an extension field.
    - CVE-2009-3563 - ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.
- 10298 – ESCVIU-126 - Access Proxy – VBP-ST – In certain conditions the access proxy firewall rules for LDAP and Presence can get out of sync with the CMA Desktop client and reports no connections to LDAP or Presence services. This issue was not easily reproduced however can exist on VBP-ST firmware prior to this fix.
    - Enhancement – The ability to view active access proxy clients was added as a link reference to the Access Proxy page.



Active Access Proxy Clients Help

Refresh Access Proxy Main Page

Current time=Thu Apr 4 20:57:32 2013

Address	Port	E164	H323-id	Device Type	Login Time	TTL
12.48.260.1	53655	408351722112	reiman1michael1HDX2	RP_DESKTOP	Thu Apr 4 20:12:00 2013	29:30

The active access proxy client displays the authenticated dynamic mode clients on the system. The list represents active client connections on HTTPS TCP port 443 from the public or Internet facing side of the system.

The list will automatically refresh in 15 seconds or select the Refresh link to immediately update the page. Access proxy updates the data read by this page every 15 seconds.

- **Address** - Displays the source IPv4 address the client is connected with for this session. When multiple clients are connecting to the system through a NAT/Firewall device several entries from the same source IPv4 address may appear. The system will sort the list by IPv4 address and port e.g. addresses that start with 1.x.x.x will be on the top of the list and addresses that start with 9.x.x.x will be on the bottom. The columns are not sortable.

- **Port** - Displays the source port the TCP 443 connection is using for this connection. When multiple clients are connecting to the system through a NAT/Firewall device multiple clients will appear with the same IPv4 address. The source port of the TCP 443 connection being used should always be different for clients with the same IPv4 address.

- **E164** - Displays the H.323 E.164 alias this client has been provisioned with to register the device's H.323 service. This information is helpful to detect this clients identity on the system and should not be used to validate the client is a registered H.323 device. Navigate to the **H.323 Clients list** page and verify this client is currently registered. The client will register this alias to the system using the H.323/H.460 RAS UDP protocol, when verifying the clients H.323 registration status the IPv4 address in this row should match the IPv4 address in the H.323 Clients list entry for this alias. However, the source ports will differ on the H.323 Client List page from the ports displayed on the Access Proxy Clients page.

- **H323-id** - Displays the H.323 H323-id alias this client has been provisioned with to register the device's H.323 service. This information is helpful to detect this clients identity on the system and should not be used to validate the client is a registered H.323

device. Navigate to the **H.323 Clients list** page and verify this client is currently registered. The client will register this alias to the system using the H.323/H.460 RAS UDP protocol, when verifying the clients H.323 registration status the IPv4 address in this row should match the IPv4 address in the H.323 Clients list entry for this alias. However, the source ports will differ on the H.323 Client List page from the ports displayed on the Access Proxy Clients page.

- **Device Type** - Displays the device type presented to the system during the authentication process. A QUASAR reference is typically associated with a CMA Desktop device.

- **Login Time** - Displays the original date and time the device authenticated to the system.

- **TTL** - **Time-to-Live** Displays the time since the clients last re-authentication or event message sent to the system. Dynamic mode endpoints send client to server message updates over the TCP 443 connection to provide endpoint statistics while in a call and heartbeat or gatekeeper registered event messages to provide status to the management server. When the system receives these messages or a re-authentication request, the TTL timer will be updated. The default system TTL is 1800 seconds or 30 minutes, some dynamic mode endpoints do not include identity information in certain status messages and will assume the default re-authentication time configured on the management server as 65 minutes. A client TTL which is incrementing down from a value of 30 or 65 and is not being reset could be considered a client which has not shutdown correctly or switched networks abruptly. When the TTL reaches 0 the system will remove any firewall access rules created when the client authenticated to the system.

- 10367 – ESCVIU-135 – H.323/H.460 – VBP-ST – When dialing outbound from an RMX MCU to a registered H.460 client on the VBP-ST some remote NAT devices did not forward the call setup to the H.460 client. When the remote H.460 client does not respond the RMX re-transmitted the call setup message, this cause the ALG to restart. Call setup re-transmissions are not common on most H.323 devices and may only be specific to RMX or other MCU platforms.

- 10421 – H.323/H.460 – VBP-ST – LifeSize endpoint support added for newer LifeSize endpoint firmware. LifeSize endpoints registering as an H.460 device require the GRQ/GFC procedure before the device will send a RRQ to register to the system. VBP-ST now sets the GCF response with a gatekeeper address of the VBP-ST Subscriber IP address or if WAN NAT has been deployed, the system will set the IP address defined on the VoIP ALG page Public NAT Subscriber IP address.

- 9927 – TLS Proxy – Internal Client – When the system is configured for internal client as LAN-side gatekeeper mode with CMA and receiving an IP only dial outbound to the Internet the call failed to route to the External VBP system for processing. This issue does not affect DMA installations; DMA and CMA have different signaling methods for IP only outbound calls.

- 10205 – H.323 – Whitelist/Blacklist – When adding a static address entry for a subnet containing 0 in the address e.g. 192.168.0.x/xx the rule was not applied correctly to the firewall.

- 10015 – H.323 – H.323 torture test discover an ALG exit if the Q.931 CalledNumber field contained "%#d%#d%#d". This issue is now resolved.

- 10606 – H.323/H.460 – VBP-ST – A network that includes a VBP-E and VBP-ST with a DMA that incorrectly routed a call initiated from a VBP-ST H.460 device, DMA forwarded the call to the VBP-E system which forwarded the call back to the VBP-ST creating a call loop

condition. When the call failed and was destroyed the ALG exited on the VBP-ST system. This incorrect call routing scenario due to a network mis-configuration will now detect a call loop condition and not allow the call.

- 9600 – Security – The following issue resolved in VOS version 11.2.13 required and additional patch to resolve the SYN case related to CVE-2004-0230. The issue resolved in VOS version 11.2.13 resolved the RST case. PCI Compliance scans may report the following issue as a PCI compliance failure – the issue is now resolved.

    - CVE-2004-0230 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS - TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

- 9882 – NTP – NTP failed to update the system time if the configured time server replied with an IPv6 response when the system was not configured for IPv6. This issue is random and depends on the time server used.

- 10591 – System – IPv6 related – When a system capable of IPv6 but is not configured for IPv6, and the WAN or LAN interfaces are installed on a network with ICMPv6 route neighbor solicitation messages present the system would halt all services requiring a reboot to recover. The issue is now resolved.

- 10562 – System – Rouser user permission – When logging into the system with the rouser user credentials the system exposed the entire UI interface to the rouser user. Depending on the platform the rouser user could view sensitive information e.g. pptp user information or the rouser user could download the system configuration on the Backup/Restore page. The rouser password was rarely changed from default which allowed anyone with knowledge of the rouser account to login to the system. The issue is now resolved by limiting the rouser UI menu access on the system as displayed below;

- 9920 – ESCVIU-120 – Access Proxy – Authentication – Certain dynamic mode Polycom clients authenticating to the access proxy on TCP port 443 caused an issue with application message fragmentation. This issue was primarily observed with CMA desktop and was limited to certain CMA desktop devices within a network solution. The issue itself has no root cause assessment however the speculation was possibly due to a workstation OS security update that modified the CMA desktop application messages and fragmented the message into 2 payloads within the same TCP packet. The access proxy was receiving 1 byte as the first payload and could not perform a security verification on this 1 byte field, the access proxy then decoded the second payload with the remaining message minus the first byte and was unable to security verification and therefor did not forward the message to CMA or Real Presence Resource manager and the connection would fail. This issue was observed on different CMA desktop client versions however appeared limited to certain workstations.

- 7719 – SIP – VBP-E - When receiving an outbound SIP invite from DMA as TCP the system performed a SIP UDP DNS SRV record query. The issue is now resolved. When the system receives a SIP UDP invite from DMA including a FQDN the system performs the following DNS lookup;

    - _sip._udp.example.com

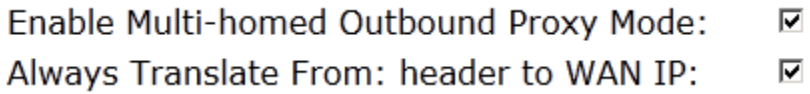
  When the system receives a SIP TCP invite from DMA including a FQDN the system performs the following DNS lookup;

    - _sip._tcp.example.com

  The DNS SRV response will/can include a single hostname or multiple hostnames with priority assignments. The system will perform a DNS A record lookup on the hostname with the highest priority and forward the call.

  The system will resolve and forward the SIP call as the protocol received from DMA e.g. SIP UDP invite will be processed and forwarded as SIP UDP. A SIP TCP invite will be processed and forwarded as SIP TCP.

- 10294 – SIP – VBP-E – Added Always Translate From: header to WAN IP on the SIP settings page. When configuring a VBP-E for SIP B2B DMA support the following UI items must be enabled on the SIP page.



- 9709 – H.323 – Neighboring – Added a Drop on WAN prefix rule to the system. This enhancement allows the administrator to drop certain WAN side calls that match a prefix entry. By adding a second prefix with an address the system will prefix route a LAN side request to the defined destination address. The system will display an H.323 Activity message when a call matching the Drop on WAN prefix rule is detected and terminated.

    - **Drop on WAN** - Setting this flag will create a policy to drop incoming WAN side calls when this prefix matches the destination string on the WAN side only. When configuring a prefix and selecting the Drop on WAN option all other fields are considered **Invalid combinations**. This feature is supported in LAN-side gatekeeper and Embedded gatekeeper modes. All other prefixes without Drop on WAN selected will be processed and routed by the system to the configured **address**.

Prefix and Gatekeeper Neighboring table

Select: All None Action: Delete

	Index	Prefix	Strip	Drop on WAN	Add	Neighbor	Local Zone	Address
☐ ▲ ▼	1	9		Yes				
☐ ▲ ▼	2	9						192.168.1.160

H.323 activity logs (newest on top)

Event/Time	Source	Destination
Call Termination	**"michael.reiman.hdx9" - 50.78.280.1**	**"95551000" - 12.48.260.1**
Apr 06 18:05:27	Duration: 0:00:00 Call-ID: 48FEF830-2057-011F-04BD-B20380B9FE5F Call-Status: Incoming Q.931 TCP connection established Termination Cause: Terminated by drop on wan prefix matching	
Alias Manipulation	**"michael.reiman.hdx9" - 50.78.280.1**	
Apr 06 18:05:27	Message: Setup (Destination Info) Modification: AnnexO Old Alias: **"95551000@12.48.260.1"** New Alias: **"95551000"**	

New Features introduced in VOS 11.2.14

- None

Fixes and Enhancements in VOS 11.2.14

- 9095 – ESCVIU-79 - Access Proxy – The VBP-E system configured to support a 2-HOP Access Proxy configuration for dynamic mode endpoint support did not allow the dynamic mode endpoints to be firmware updated when a new firmware version was available from the CMA management server.

- 9770 – H.323 – LifeSize Interoperability – Newer models of LifeSize endpoints include a source alias type as TransportID that contains the endpoints configured IP address. When calling through a VBP-E configured for Embedded Gatekeeper or LAN-Side Gatekeeper this field was not modified to the VBP's public address. The called endpoint reacted to this source alias type and attempted to contact this private IP to continue call processing and the call failed. This source alias type is not widely used in the industry and until further investigation of the fields intended usage is clearly defined, the VBP will remove this source alias type from the call setup message. All standard destination alias types in the setup message will not be modified this change only applies to a source alias type set as TransportID and contain an IP address.

- 9903 – Access Proxy – Re-exposed the Access Proxy feature for Russian Federation ordered products.

New Features introduced in VOS 11.2.13

- None

Fixes and Enhancements in VOS 11.2.13

- 9543 – Security – OpenSSL – In version 11.2.12 – 9246 - OpenSSL 1.0.1c was integrated to address confirmed CVE's. The system supports two embedded root certificates from VeriSign and Go-Daddy to support certificate chaining. The Go-Daddy root CA was not moved forward during the OpenSSL integration performed in 11.2.12. This is now resolved.

- 9592 – ESCVIU-109 – System – VBP-E - FTP User – The system File Server feature allows a user to enable FTP or TFTP functionality, this feature is commonly used to capture system debug file and allows the user to create a username/password to login and transfer these files to their local computer. The FTP user feature was unable to create a new user. This issue is now resolved.

- 9575 – ESCVIU-113 – TLS Proxy – Internal Client – When the VBP is configured for TLS Proxy and the Internal Client is configured for the Embedded Gatekeeper the system was not processing destination IP only dialed calls through the tunnel to the external system for outbound call processing. ANNEX O dialed destinations worked as expected.

- 9600 – Security – PCI Compliance scans may report the following issue as a PCI compliance failure – the issue is now resolved.

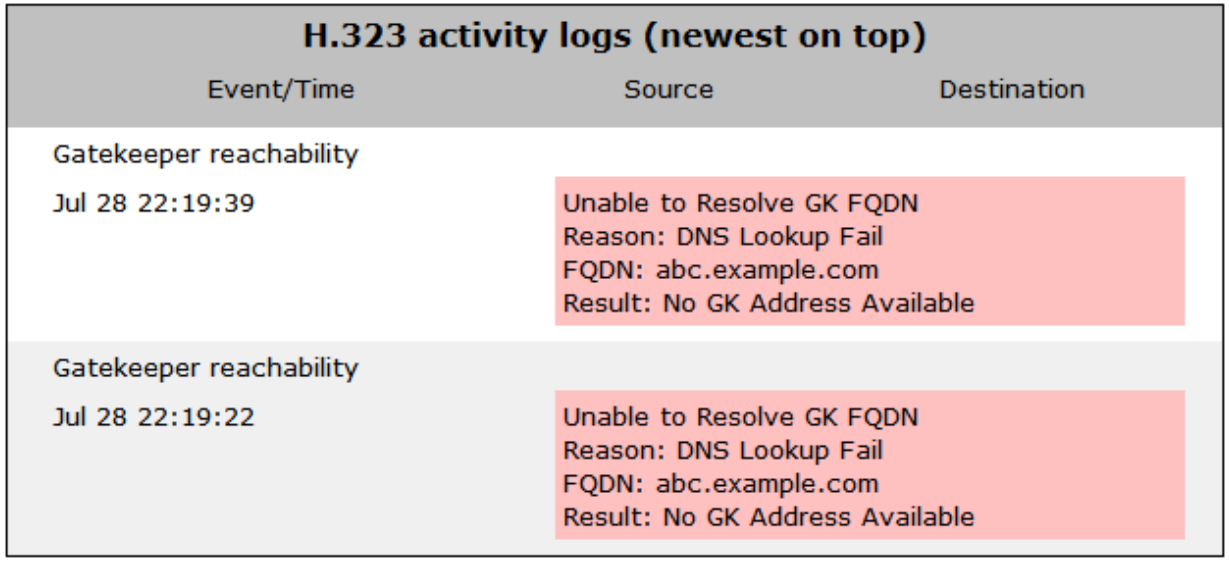
    - CVE-2004-0230 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS - TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.

- 9601 – Security – PCI Compliance scans may report the following issue as a PCI compliance failure – the issue is now resolved.

    - CVE-2011-3188 - Linux Kernel TCP Sequence Number Generation Security Weakness - The (1) IPv4 and (2) IPv6 implementations in the Linux kernel before 3.1 use a modified MD4 algorithm to generate sequence numbers and Fragment Identification values, which makes it easier for remote attackers to cause a denial of service (disrupted networking) or hijack network sessions by predicting these values and sending crafted packets.

New Features introduced in VOS 11.2.12

- 7881 – H.323 – VBP-E – FQDN support for LAN-side Gatekeeper Mode – The system now supports entering an FQDN or an IPv4 address as the LAN-side gatekeeper address. When an FQDN address is configured the system will perform an h323_cs SRV query then, A record query to resolve the FQDN. If the FQDN is entered incorrectly or the systems DNS server is unavailable the following Activity log message will be displayed;



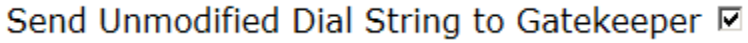
H.323 activity logs (newest on top)

Event/Time	Source	Destination
Gatekeeper reachability		
Jul 28 22:19:39	Unable to Resolve GK FQDN Reason: DNS Lookup Fail FQDN: abc.example.com Result: No GK Address Available	
Gatekeeper reachability		
Jul 28 22:19:22	Unable to Resolve GK FQDN Reason: DNS Lookup Fail FQDN: abc.example.com Result: No GK Address Available	

The system performs a query at 15 second intervals for the configured FQDN, with a successful A record response the system will use the first priority 1 A record address to forward H.323 calls. If the DNS server becomes unreachable after a successful lookup has occurred the system will continue to use the last known priority 1 A record address until the DNS server becomes reachable.

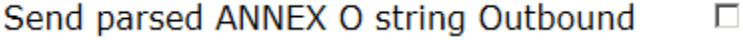
- 8823 – License Key – H.323 – Added support for a 50Mbps license key

- 9053 – ESCVIU-98 – H.323 – VBP-E LAN-side gatekeeper mode – When receiving an ANNEX O dialed string e.g. user@host on the WAN interface the system previously modified the message and forwarded only the user portion to the configured gatekeeper address for call processing. The following check box has been added to the LAN-side gatekeeper mode settings to allow the full unresolved ANNEX O string to be sent as received to the gatekeeper for call processing.



- 9206 – ESCVIU-98 – H.323 - VBP-E LAN-side gatekeeper mode or Embedded gatekeeper mode – In pre 11.2.x version of VBP VOS when the user dialed string of user@host was dialed by a LAN side endpoint behind a VBP the system would modify the string and only send the user portion to the destination system. Post 11.2.x VBP VOS will send the full ANNEX O string to the destination system as it was dialed by the LAN side endpoint. Noted in VOS release 11.2.6 with issue 6934 the older VBP VOS 7.2.2 configured as Embedded gatekeeper was unable to provide call processing when the full unresolved ANNEX O string was received. In certain solutions with older VBP VOS it may be desired to revert the outbound ANNEX O user@host string to be modified and sent as the user portion only. This option is only needed when dialing ANNEX O destinations to VBP VOS 7.2.2 from VBP VOS 11.2.x systems.

  By enabling the following option the system will modify the outbound ANNEX O string to only send the user potion to the destination system.



Fixes and Enhancements in VOS 11.2.12

- 8656 – H.323 – Whitelist/Blacklist - VBP-ST – Enhanced the existing feature to support Polycom dynamic mode endpoints. When the system is configured for Whitelist Static/Dynamic all H.323/H.460 requests to UDP port 1719 and TCP port 1720 will be dropped unless defined.

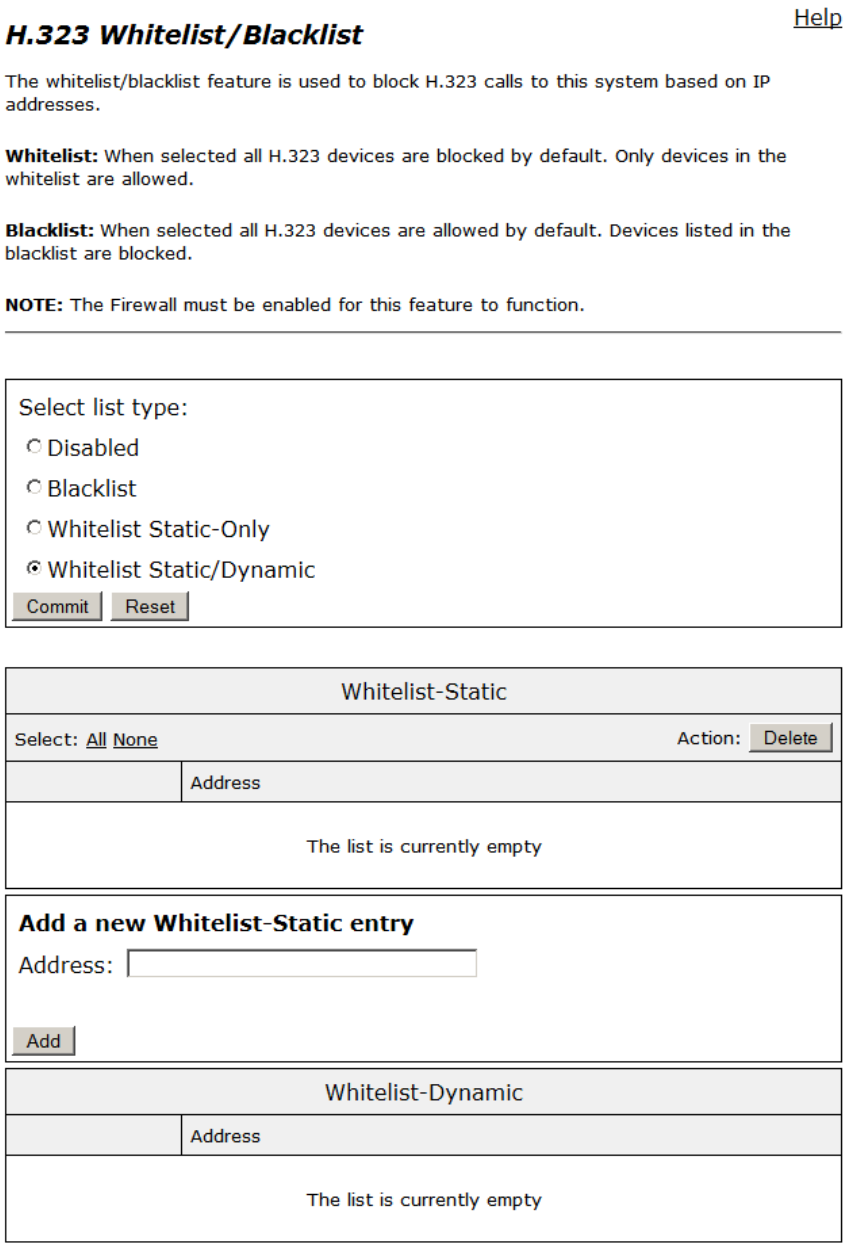
  Dynamic mode endpoints are supported today through the Access Proxy, this feature enhancement now includes automatic UDP 1719 and TCP 1720 rule insertion from these authorized endpoint source IP's for registration and call setup. All other source IP's will be dropped. When supporting H.323/H.460 endpoints that do not support dynamic mode authorization a Whitelist-Static entry must be entered.

  When enabling the Whitelist Static/Dynamic operation mode, the system automatically adds currently authorized dynamic mode endpoints to the rules. Static entries will need to be added manually for non-dynamic mode endpoints.

  Adding a Whitelist or Blacklist static entry will not disrupt ongoing calls.

  The feature now supports changing from Disabled to Whitelist Static/Dynamic or any combination of setting without disrupting current calls.

  The ability to add a Whitelist/Blacklist static entry for a DNS name is not supported with this release.



- 9304 - H.323 – Whitelist/Blacklist – Modified the feature to accept a bit mask when configuring a static entry. The static entry can now be configured as a host addresses e.g. a.b.c.d or subnet in bit mask format a.b.c.d/xx.

- 8540 – ALG - H.323 – TLS Proxy - DMA interoperability – Destination IP only calls from DMA when the VBP-E is configured in TLS Proxy mode e.g. when the user dials an IPv4 only call destine for a public IP endpoint via the DMA configured VBP-E system used for B2B calling the call will fail to be processed correctly by the VBP-E system. This issue is now resolved.

- 9246 – Security – OpenSSL – Updated OpenSSL to version 1.0.1c to address the following CVE's

    - CVE-2011-3389 - SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Vulnerability
    - CVE-2011-1923 - SSL/TLS server accepts a weak Diffie-Hellman public value
    - CVE-2012-2333 - OpenSSL Security Advisory 20120510

- 6384 – VoIP Traversal – VoIP traversal Firewall – Added additional fields to the VoIP Traversal Firewall settings. The system can now support the ability to add a port range, and packet type (TCP/UDP/ANY) to VoIP Traversal firewall rules. Additional error checking was added to help prevent duplicates, and to verify the port range is correct.

    - 6909 – VoIP Traversal – VoIP traversal Firewall – Added warning messages, and disallowed enabling the VoIP Traversal Firewall if the main system firewall is off. Added a warning message on the main system firewall page, and the VoIP Traversal Firewall page, if the main system firewall is off, and the VoIP Traversal firewall is on. Also, if both are off, the VoIP Traversal firewall can no longer be enabled until the main firewall is back on.

- 8189 – VoIP Traversal – VoIP traversal Firewall – If a port was specified when adding VoIP traversal firewall rule the rule would not be added correctly in iptables.

- 9239 – VoIP Traversal – Remote client – The VBP-E configured as a VoIP Traversal remote client allows a LAN side device to request DHCP to obtain a VoIP Traversal network IP address. The LAN side device did not receive the correct routes in the DHCP offer.

- 9010 – Security – VBP-ST – The UI option to configure Trusted Host in the Security menu had been incorrectly removed from the UI.

- 9013 – ALG – CDR logs – Enabling CDR logs did not warn the user that call disruption would occur when enabling this feature. The system now warns the user with the following message; **`WARNING: All voice and video services will be interrupted. Do you want to continue?`**

- 9093 – ESCVIU-95 – User Management – When User Management is enabled the ROUSER user account password was not able to be changed. The ROUSER account is now disabled when User Management is enabled.

- 9094 – ESCVIU-94 – H.323 – Clients list – Modified the system to allow a dynamically registering endpoint to be locked as a permanent client. This modification allows a dynamically registering endpoint to also unregister and then re-register from the Embedded gatekeeper with a locked client. The dynamically registering endpoint must re-register from the same IP and the same H.323 RAS ports. The Polycom

m100 client cannot be supported at this time because the source ports are assigned dynamically by the computer and may change when the m100 client is shut down and restarted.

- 9207 – ESCVIU-101 – Access Proxy – LDAP – VBP-E 2 Hop - In certain CMA deployments LDAP directory searches failed when deployed behind a remote location VBP-E Access Proxy configured to proxy to the headquarters VBP-ST. This issue is now resolved.

- 9215 – ESCVIU-100 – GUI – Internet Explorer version 8 and 9 when connecting to the system could take up to 2 minutes to receive a login. The issue is now corrected.

- 9262 – Stateful Failover – VBP-E – Port Forwarding – When creating a Port Forwarding rule on the VBP-E system with Stateful Failover enabled, the WAN Interface IP token HA_VIP was not adding the correct rules to allow the port forwarding rule to function as designed.

- 9319 – ALG – H.323 – Modified all H.323 timers and enabled Stale Time by default. Field deployed systems with these values configured as non-default settings will not be modified, systems that are factory defaulted will use the new timer settings as defined below;

  VBP-ST - Provider gatekeeper mode
  Modify Time-To-Live: Checked
  Time-To-Live (s): 30
  Delete stale clients: Checked
  Stale time (m): 1
  H.460.18 Support
  Keep-alive time (s): 30

  VBP-E – WAN-side gatekeeper mode
  Delete stale clients: Checked
  Stale time (m): 1

  VBP-E - Embedded gatekeeper mode
  Time-To-Live (s): 30
  Delete stale clients: Checked
  Stale time (m): 1

  TLS Proxy – VBP-E Internal client - Forwarding gatekeeper mode
  Modify Time-To-Live: Checked
  Time-To-Live (s): 30
  Delete stale clients: Checked
  Stale time (m): 1

- 9320 – WAN NAT – VBP-E – VBP-E system configured to support the WAN NAT feature deployed in a private DMZ received an ANNEX O inbound call as user@PUBLIC_NAT_IP. Certain gatekeepers require the ANNEX O message to be modified to only send the user portion. In previous VBP-E logic the system automatically removed the host portion if the IP matched the VBP-E's configured WAN IP address. With the system deployed in a NAT-ed environment the actual VBP-E WAN IP address no longer matched the incoming H.323 URI therefor the system forward this user@PUBLIC_NAT_IP address and call processing will fail if the gatekeeper cannot resolve this address.

- 9349 – TLS Proxy – Internal Client – The recent race pacing feature modification performed in VOS 11.2.10 defined as issue 8622 created a client's list synchronization issue between the external and internal VBP's configured in TLS Proxy mode. TLS Proxy configurations must use the new H.323 timers discussed in issue 9319 to ensure the H.323 clients list remain synchronized.

- 8884 – ALG – H.323 – VBP-ST – The H.323 ALG may restart when certain network delay conditions exist with Real Presence Mobile Android tablets.

New Features introduced in VOS 11.2.10

- 8737 – ALG – H.323 WAN/LAN NAT – The system can now be installed behind a perimeter security NAT device. This allows incoming traffic to the public IP to be translated to the systems internal IP. This is typically called a private DMZ which allows devices in this DMZ to be configured with a private RFC1918 IPv4 address. The NAT configuration must be a Public IPv4 address configured for a one-to-one NAT translation without any port-mapping to the VBP-ST or VBP-E internal DMZ Subscriber/WAN IPv4 address.

- 8622 – ALG – H.323 – VBP-ST – Provider Gatekeeper performance enhancement - Rate pacing for keep-alive WAN traffic. The VBP-ST system will now rate-pace all keep-alive (or light-weight) RRQs sent from endpoints. The VBP-ST system will respond locally to this keep-alive traffic and will not forward this traffic to the Provider side gatekeeper.

  The VBP-ST system will send a single keep-alive RRQ to the Provider gatekeeper at 50% of the gatekeeper TTL interval e.g. the default TTL for registration refresh interval is 300 seconds. The VBP will send a keep-alive at 50% of the TTL value or every 150 seconds. This reduces the keep-alive RRQ load on the Provider gatekeeper instead of forwarding one keep-alive RRQ for each endpoint registered to the VBP-ST.

  When the endpoint sends an additive RRQ, a full RRQ, or a URQ, the VBP-ST will forward the message to the gatekeeper in order to keep the VBP-ST and gatekeeper client registration state in synch. The feature is only enabled on ST systems in Provider gatekeeper mode.

- 8199 – VoIP Traversal – TLS Proxy mode – The system can now be configured in TLS Proxy mode or TLS Routed mode depending on the solution requirements. TLS Proxy mode allows the system to proxy the application traffic as the configured VBP Public or Private interface IP's and removing the routed subnet requirement.

- 8067 – System – 6400LF2 – Removed all applications that allow a remote client to connect to the VBP that encrypt the session for transferring data to/from the remote network and to/from the core or headquarters network. This is a requirement for shipping VBP systems to Russia. A Russian part number must be order to have the system built with no encryption. Encrypted management session e.g. HTTPS, SSH are allowed to manage the system, these management applications will function as normal.

  - 8061 – GUI – 6400LF2 – The model name of this platform was changed to 6400LF2 and only if a disable encryption license key is applied. This was modified for homologation requirements.

Fixes and Enhancements in VOS 11.2.10

- 8026 – ESCVIU-78 – H.323 – Calls to the default alias failed to route in certain origination scenario's

- 8387 – ALG - H.323 – DMA interoperability – DMA 4.0.1_build_4 version configured for a VBP-E for outbound dialing included a transportID field in the call setup message as the destination IP dialed by the user. This message type was not parsed or removed correctly by the origination VBP-E or the destination VBP-E

- 8565 – ALG – H.323 – DMA interoperability – When a VBP-ST registered endpoints unregisters from the VBP-ST configured for a DMA gatekeeper the VBP-ST send a URQ request to the gatekeeper to unregister the endpoints aliases. DMA now removes all known aliases for the VBP-ST Provider IP address and responds to the next keep-alive RRQ as "Full Registration Required". This message indicates to the VBP-ST system that the gatekeepers registered clients list is no longer synchronized with the VBP-ST clients list. The VBP-ST now initiates an auto-registration cycle to re-synchronize the VBP-ST clients to the gatekeeper.

  The VBP-ST will send an RRQ request to the gatekeeper one alias pair at a time and wait for a RCF response. During this process if a network delay condition exists, for example greater than 1 second delays and the VBP-ST is still receiving full RRQ's on the Subscriber interface to re-register. The VBP-ST will initiate multiple auto-registration process and eventually cause the ALG to exit. This condition is now resolved by not allowing the auto-registration process to execute more than one instance.

- 8630 – ALG - H.323 – DMA interoperability – The current DMA design allows calls to Inactive endpoints, when a VBP-ST registered endpoint calls this Inactive endpoints destination alias the DMA re-directs the call to this endpoint. If this endpoint is currently registered to another gatekeeper on the network the active gatekeeper will signal the endpoint to send a facility message "route call to gatekeeper" the VBP-ST ALG exits in this condition if the releaseComplete arrives before the setup message has been forwarded to the endpoints currently registered gatekeeper. This issue has only been observed if certain network conditions exist, this issue is now resolved.

- 8629 – ALG - H.323 – DMA interoperability – In certain gatekeeper RAS conditions "caller not registered" the VBP-ST incorrectly formatted the RRJ message and was not sent to the client.

- 8538 – ESCVIU-85 – Security – Certificate Store – The system would not allow the creation of a certificate with a hyphen included in the Common Name field. The system has been modified to support domain name characters per RFC952 - alphabet (A-Z) (a-z), digits (0-9), hyphen, period, and underscore

- 8636 – GUI - Web Server – Some web browsers send HTTP GET requests in multiple packets e.g. Chrome and some versions of IE. When using these web browsers the VBP web server processes this as two separate requests and resets the connection.

- 8657 – ESCVIU-84 - System – Kernel – 6400LF2 only - When the 11.2.x release was under development for the kernel port to linux 2.6.33, kernel logging was enabled and was left enabled when VBP VOS 11.2.3 was released. In certain conditions e.g. the system logging firewall messages created by the VBP's TCP connection limits 10/sec burst 20 caused a significant amount of traffic on the console port. This traffic caused the console driver to access and busy out all 4 CPU's in the quad core system. This resulted in the

systems inability for other applications to obtain CPU interrupts for processing and has the appearance of all services halting while this traffic condition exists. Kernel logging is now disabled on the 6400LF2 system.

- 8825 – ALG - H.323 – RTP port array – Noted below, the 9.1.5.x documented ports for all platforms were inadvertently changed to increase supported calls on the system. This change also modified the systems ALG RTP port array when 11.2.x was released to increase call capacity and was not documented correctly in the VBP configuration guide. This version modifies the ALG RTP array back to the documented values. This has no effect on the current system supported call values; this increased call modification made was for future scalability reasons.

    - 9.1.5.x releases

        - 16386 - 17286 (200EW,4300,4350,4350EW) (contiguous range)
        - 16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
        - 16386 - 34386 (6400-E and S85) (contiguous range)

    - 11.2.3 to 11.2.9

        - 16386 - 17286 (200EW,4300,4350,4350EW,4555) (contiguous range)
        - 16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
        - 16386 - 52386 (5300LF2-E/S10 and E/S25) (contiguous range)
        - 16386 - 52386 (6400-E and S85) (contiguous range)

    - 11.2.10

        - 16386 - 17286 (200EW,4300,4350,4350EW,4555) (contiguous range)
        - 16386 - 25386 (5300-E/S10 and E/S25) (contiguous range)
        - 16386 - 25386 (5300LF2-E/S10 and E/S25) (contiguous range)
        - 16386 - 34386 (6400-E and S85) (contiguous range)

- 1043 – ESCVIU-81 – H.323 – When adding static H.323 clients or locking a dynamic client in the list, the system did not save these changes which resulted in the client being deleted if the system was restarted.

- 8182 – H.323 – Whitelist/Blacklist – Modified the feature to allow new rule entries to not interrupt ongoing calls. If the administrator changes from Whitelist to Blacklist or Blacklist to Whitelist this action will be disruptive to ongoing calls.

  Modified the feature for the VBP-ST to include RAS UDP 1719 to the block/allow rule set. Example: If the blacklist feature is enabled all remote H.323/H.460 clients will be able to register to the system. Adding a source IP to the blacklist will now add firewall rules to DROP RAS UDP 1719 from this source IP only. If the whitelist is enabled all remote H.323/H.460 RAS UDP 1719 client requests will be dropped and only the defined remote IP's will be allowed to register to the system.

- 8266 – GUI – H.323 – Activity, Call Status and VoIP ALG pages – minor wording changes

  Previous GUI language;
  Current payload bandwidth:
  Estimated total bandwidth:

  Changed to
  VoIP ALG Licensed Bandwidth In Use:
  Current Total Bandwidth With IP Overhead:

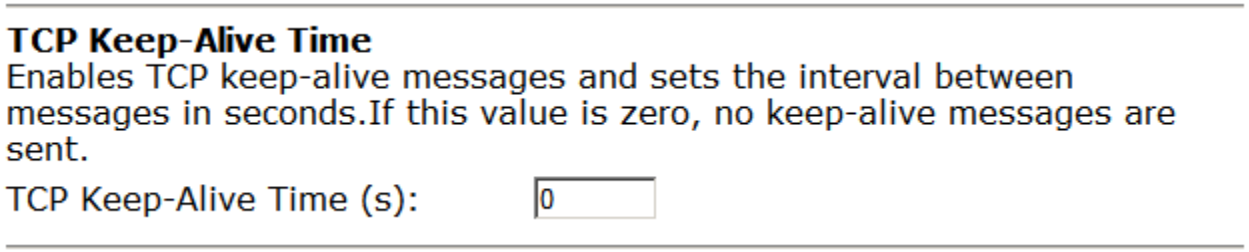
- 8259 – H.323 – DMA – VBP-ST interoperability with H.460 Subscriber side clients when the DMA is configured for an H.323 auto call model to select a routed or direct call. When calling from a Subscriber H.460 enabled endpoint to a Provider side endpoint the call was failing due to the direct call model with a H.460 endpoint.
  - 8322 – H.323 – DMA – VBP-ST interoperability with H.460 Subscriber side clients calling Provider side clients in a direct call model. The system was not translating the destCallSignalAddress correctly.
- 7788 – Security – Disabled SSLv1 and SSLv2 and removed weak ciphers from the system.
- 7816 – VoIP Traversal – LDAP – VoIP Traversal Authentication configured as LDAP would not accept an IP address entry.
- 7844 – ESCVIU-76 – Stateful Failover – Access Proxy failed to process requests after a reported 4hr time frame.
- 7916 – ESCVIU-77 – Firewall Logging – The Enabled Firewall Logging check box would not stay enabled after a submit.
- 7977 – VoIP traversal – A side effect of adding Vlan support for TLS in VOS version 11.2.6 – 7356 - would not allow the TLS Remote Client to use the default LAN interface for TLS traffic if Vlans were not enabled.
- 7749 - ESCVIU-75 – Access Proxy – Signed Certificates as the Subscriber Certificate – The system would use a signed certificate as the Subscriber Certificate but did not chain to the certificate authority (CA) correctly. Currently the system support 2 root CA certificates for certificate chaining, VeriSign and Go-Daddy. This modification allows the user uploaded VeriSign or Go-Daddy signed certificates to chain to the root VeriSign or Go-Daddy root CA preinstalled on the system. Currently the system does not allow the user to upload and use a different root CA.

New Features introduced in VOS 11.2.6

- 7356 – VoIP Traversal - TLS Traversal remote client - VLAN capable and Access Proxy Added the ability to configure the LAN side of the Access Proxy to one VLAN, and the LAN side of the VoIP Traversal client to another VLAN. Reference the 11.2.6 VBP Configuration guide to configure the system.

- 6650 - ESCVIU-65 – H.323 – TCP keep-alive – In certain VBP deployments remote H.323 devices may be installed behind non VBP security appliances that monitor TCP connections for activity. In this scenario the security appliance may close the TCP connections between the far end VBP and the remote endpoint causing the call to drop. Setting the TCP keep-alive feature forces the endpoint to create a keep-alive packet on TCP connection's to the VBP for H.323 connections at the interval time set in the configuration file.

    - 7147 – EXT-4141 - Add a TCP keep-alive feature to H.323 page. Added a GUI option for TCP keep-alive for H.323 TCP connections. The minimum time is 120 (s)



- Example /etc/config/alg_defs.conf file

```
MGCP_CALLAGENT_IP=0.0.0.0
MGCP_CALLAGENT_PORT=2727
MGCP_MEDIAGATEWAY_PORT=2427
MGCP_NOTIFIEDENTITY_PORT=2432
SIP_CALLAGENT_IP=0.0.0.0
SIP_PORT=5060
GK_IP=12.48.260.19
SCCP_IP=0.0.0.0
TFTP_IP=0.0.0.0
SIP_SHARED_DIDS=off
MGCP_ASTERISK_PORT=6727
LAN_ALG_IP=192.168.1.1
ALG_VLAN=eth0
H323_GKMODE=3
H323_LANGK=
```

H323_GK_TTL=300
H323_MAX_ALIASES=0
H323_MOD_TTL=off
H323_TTL=300
H323_USE_MCAST=off
H323_STALEURQ=off
H323_STALEURQ_TIME=60
H323_NOTRAN_LCF=off
H323_DEF_ALIAS=7221
H323_DEF_ALIAS_TYPE=0
H323_NATTRAV=2
H323_NATTRAV_TIME=45
H323_PREVENT_UNREG=off
H323_LRQ_SIZE=off
H323_GK_ROUTED=off
H323_Q931_PORT=1720
OPTION=""
H323_TCP_KEEPALIVE_TIME=120

Fixes and Enhancements in VOS 11.2.6

- Correction on VBP VOS 9.1.5.3 release note – License key – Support for 200Mbps of video on the 6400 platform only. The 200Mbps license key support is for the 6400LF2 platform only.

- VIDEO-93593 - HDX endpoints configured for dynamic management using the VBP-ST Access Proxy might not upgrade correctly under certain conditions when the HDX system is behind a remote NAT network environment. HDX software version 3.0.3 resolves this issue by supporting authenticated upgrades. HDX systems must first be manually updated to version 3.0.3. After the HDX is upgraded to version 3.0.3 future upgrades can be managed by the CMA server by the administrator.

- 5201 - ESCVIU-71 – 6400LF2 - VBP VOS 11.2.3 included a Linux kernel update from 2.4.24 to 2.6.33. 6400LF2 platforms have a storage device mounted by an internal USB controller, this device was randomly un-mounting itself and then re-mounting the USB attached storage device. The system could not re-mount the USB device successfully causing loss of GUI and SSH access to the system. After some period of time new H.323 registering systems and or H.323 calls will fail to be processed by the system. Updated the Linux USB device drivers to address this issue on 6400LF2 platforms only.

- 7002 – ESCVIU-68 – H.323 – This issue was a side effect from resolving bandwidth down speeding addressed in VOS version 11.2.3 - 5967 – ESCVIU-45. When LAN to LAN calls were placed and the system was in Embedded gatekeeper mode, the system sent a BRJ for the call with no currents calls being processed by the system. LAN to WAN calls were being process correctly, the issue only happen on LAN to LAN calls. This issue also affected WAN-side gatekeeper mode.

- 6528 – Security – Updated the SSH daemon to OpenSSH version 5.8p2

- 7521 – VIU-203 – License key – Display S or ST on the System page based on license key The system now displays S or ST based on H.460 license key.

- 6582 – ESCVIU-64 – Access Proxy - H.323 Needs the ability to enter FQDN within the CMA address field It is now possible to enter an FQDN in the server field for access proxy configuration. The access proxy will do an A lookup on the FQDN and use the resulting address with the configured port number to forward requests.

- 6934 - ESCVIU-70 – CMA 5.5 and VBP-E 9.1.5.3 dialing into Tandberg expressway hosting multiple domains does not work as the VBP is stripping the domain from the call setup.

  This case is linked or duplicates of EXT-4046 and ESCVIU-67

  Logic change: The user dialed string of user@host in any combination alias@IP or alias@domain sent from the endpoint in the ARQ to the Embedded Gatekeeper will be first resolved and then sent unmodified in the SETUP to the destination in the same field received in the ARQ. Since this field is sent by the endpoint (typically an h323-ID) the forwarded SETUP to the destination will also be the h323-ID.

When VBP's in the field are upgraded to this version and future versions, calls from VBP's with this version to older VBP versions is as follows.

Embedded Gatekeeper
VBP VOS 7.2.2 – will not receive user@host dialed strings unless an alias manipulation rule of @VBP_WAN_IP is configured.
VBP VOS 9.1.5.1 – Will receive user@host dialed strings
VBP VOS 9.1.5.3 – Will receive user@host dialed strings
VBP VOS 11.2.3 – Will receive user@host dialed strings

LAN Side Gatekeeper
VBP VOS 9.1.5.1 will strip the @VBP_WAN_IP_or_DNS before sending it to CMA – this logic has not changed
Calls from CMA with the unresolved string will be forwarded to the destination in the same field CMA sends the SETUP to VBP.

- 7084 – Access Proxy – VBP-E 2Hop – VBP-E Access Proxy with CMA when integrated with active directory using longer than expected user strings – Users were not able to login with active directory accounts, local accounts authenticated correctly – Dynamic mode provisioning message over 8190 bytes where not forwarded correctly - minor changes to buffering of provisioning messages over 8k was introduced.

New Features introduced in VOS 11.2.3

- TLS VoIP Traversal – System – Added support for TLS Traversal as a new networking method for the VBP using a single UDP TLS port for traversal through the existing enterprise NAT/Firewall and a remote TLS VBP client for connecting remote branch office video systems to the core UC info-structure. This feature includes support for a legacy VBP-ST that is installed on the WAN/LAN (Subscriber/Provider) interfaces to connect remote branch office locations with a remote VBP-E TLS Traversal client.

- IPv6 – Network – Added support for IPv6 on the 4555, 5300LF2 and 6400LF2 platforms.

- HTTPS – Management – Added default HTTPS certificates for all platforms for management to the system.

- Certificate Store – System – Added the ability for the system to create CA, TLS Server, TLS Client, CSR and HTTPS certificates.

- User and Session Management – The system now support the ability to create non root user accounts. The system administrator can now create specific user accounts with administrator or auditor privileges. Administrators will have full access to the system, and auditors will only have privileges to view and clear and download audit logs.

- Audit Logging – System – Added support for the system to track configuration changes for any uses perform configuration changes to the system.

- 4999 – NAT – Added NAT support on a VBP-E system when configured in VRRP. The system will now accept the token name VRRP_VIP as the Src IP field in the NAT statement. This token will only apply the NAT statement to the VRRP VIP IPv4 address for the WAN interface on the acting MASTER system.

Fixes and Enhancements in VOS 11.2.3

- 6975 – Resolved a memory allocation issue in the Access Proxy process. A symptom of this issue could be seen as “Signing into Presence Server” on CMAD clients. If Access Proxy used all available memory, the process would restart and self recover in approx 15 seconds. Any CMAD client requesting Access Proxy services during this period would report the service as down and then re-authenticate. H.323 services would not be interrupted.

- 5967 – ESCVIU-45 – GUI – VBP now calculates the correct bandwidth usage when the H.323 device down speeds the bandwidth during the call from the initial requested call speed. This fix addresses the following configuration modes:

    - VBP-E Embedded Gatekeeper
    - VBP-E WAN side Gatekeeper
    - VBP-ST Provider Side Gatekeeper

- 6650 – ESCVIU-65 – H.323 – TCP keep-alive – In some installations the far end NAT router that is configured with or without a remote VBP my close the 1720 TCP port because of no activity and causing the call to drop. TCP keep-alive forces the remote client to send TCP keep-alive packets on port 1720. A new entry in the configuration file is needed to enable this support, a GUI option is not available at this time.
    - H323_TCP_KEEPALIVE_TIME=120 (value in seconds 120 or greater) to the etc/config/alg_defs.conf file

- 6540 – ESCVIU-63 – Ethernet Drivers – During video calls with a bandwidth throughput of 30Mbps packet @ 4700-5000 packets per second or greater, occasional packet loss is experienced on RX side of the interfaces. This issue is only experienced on the 6400LF2 platform. Disabling NAPI within the driver resolved this issue.

- 4628 – ESCVIU-34 – Security – VBP 9.1.5.3 and prior version had a maximum 8 character GUI password length, with the new User and Session management feature the password length is 32 alpha, numeric, special characters supported.

- 5891 – ESCVIU-52 – GUI – Minor wording changes in the GUI

- 5233 – ESCVIU-43 – Firewall – Management Interface – The VBP-E system was incorrectly responding to management protocols on the LAN interface with the management interface configured if the radio buttons on the firewall page where unchecked. The workaround to this issue was to check the management protocols on the firewall page and LAN access to the system is now blocked and only traffic from the management subnet is allowed.

- 5670 – ESCVIU-44 - H.323 – WAN Side gatekeeper mode – Interoperability between a RadVision gatekeeper and a Tandberg endpoint with a VBP-E configured in WAN Side gatekeeper mode. The VBP-E was removing the clients alias list when the Tandberg endpoint sent a Keep-alive RRQ and the Radvision gatekeeper had not signaled support for keep-alive RRQ causing the Radvision gatekeeper to remove the endpoint from the registered clients list.

- 5815 – ESCVIU-46 – H.323 – Embedded gatekeeper – This is related to issue 1463 - ESCVIU-27 – H.323 – Support for FACILITY – The Embedded gatekeeper now includes the destinationAddress in the redirected call SETUP

- 6006 – ESCVIU-55 - Access Proxy – Enabling the Access Proxy and changing the admin password on 5300LF platforms only would cause the GUI to stop responding. This issue would not cause a service interruption.

- 6126 – ESCVIU-58 – H.323 – H.460 – H.460.19 uses a RTP keep-alive payload type used for keeping the NAT router connection tracking entries alive, these RTP payload types should be dropped at the VBP-ST traversal server and not forwarded to the remote client. This issue is related to improving H.460 traversal with certain NAT routers as 5234. The system was not dropping these RTP payload types to the remote client and in some cases causing the remote client to reboot.

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 performed 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 approximately 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.

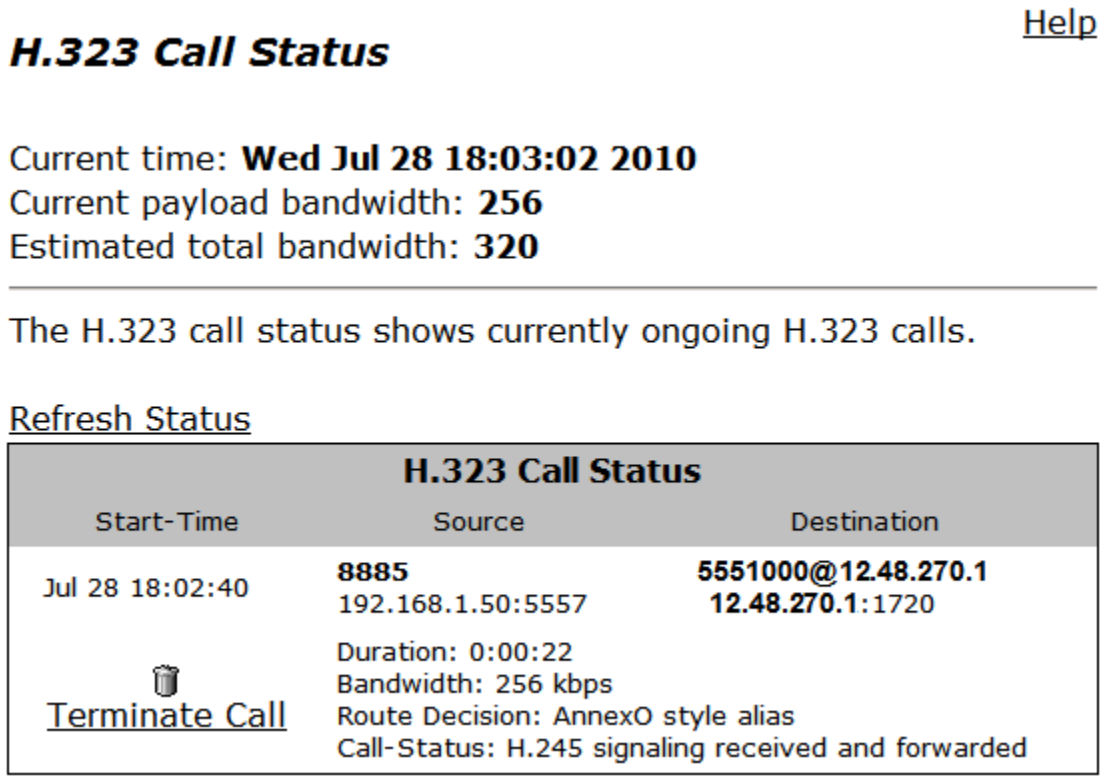
  The default setting on a VBP-E system registered client can take up to 300 seconds or 5 minutes to re-register.

- 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 6400LF2 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	

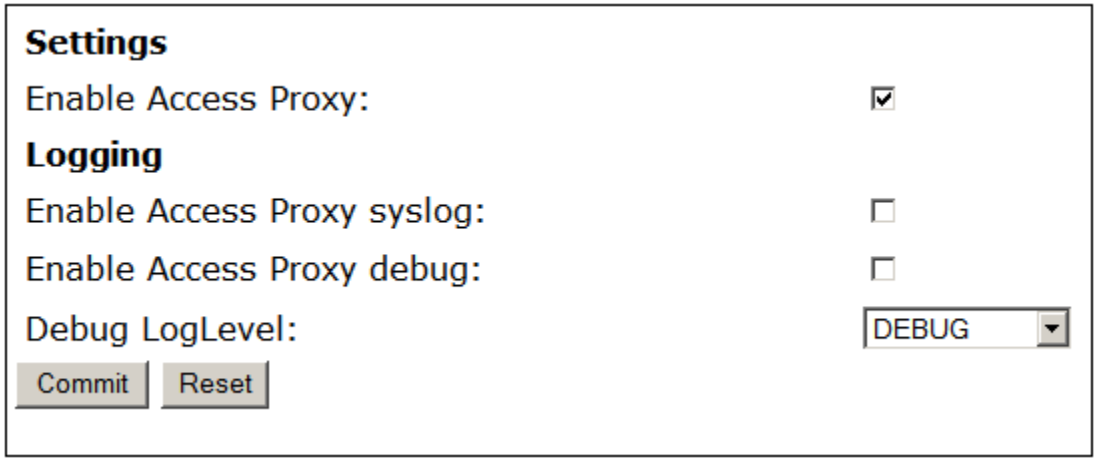
Fixes and Enhancements in VOS 9.1.5.3

- 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.

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.

END-USER LICENSE AGREEMENT FOR POLYCOM® SOFTWARE

IMPORTANT-READ CAREFULLY BEFORE USING THE SOFTWARE PRODUCT:

This End-User License Agreement ("Agreement") is a legal agreement between you (and/or any company you represent) and either Polycom (Netherlands) B.V. (in Europe, Middle East, and Africa), Polycom Hong Kong, Ltd. (in Asia Pacific) or Polycom, Inc. (in the rest of the world) (each referred to individually and collectively herein as "POLYCOM"), for the SOFTWARE PRODUCT licensed by POLYCOM. The SOFTWARE PRODUCT includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By clicking "I AGREE" or by installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be and will be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, your use is prohibited and you may not install or use the SOFTWARE PRODUCT.

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed (not sold) to you, and its use is subject to the terms of this Agreement. This is NOT a sale contract.

1. GRANT OF LICENSE. Subject to the terms of this Agreement, POLYCOM grants to you a non-exclusive, non-transferable, revocable license to install and use the SOFTWARE PRODUCT solely on the POLYCOM product with which this SOFTWARE PRODUCT is supplied (the "PRODUCT"). You may use the SOFTWARE PRODUCT only in connection with the use of the PRODUCT subject to the following terms and the proprietary notices, labels or marks on the SOFTWARE PRODUCT or media upon which the SOFTWARE PRODUCT is provided. You are not permitted to lease, rent, distribute or sublicense the SOFTWARE PRODUCT, in whole or in part, or to use the SOFTWARE PRODUCT in a time-sharing arrangement or in any other unauthorized manner. Further, no license is granted to you in the human readable code of the SOFTWARE PRODUCT (source code). Except as expressly provided below, this License Agreement does not grant you any rights to patents, copyrights, trade secrets, trademarks, or any other rights in respect to the SOFTWARE PRODUCT.

2. OTHER RIGHTS AND LIMITATIONS.

2.1 Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, modify or disassemble the SOFTWARE PRODUCT or otherwise reduce the SOFTWARE PRODUCT to human-perceivable form in whole or in part, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one PRODUCT. You may not use the SOFTWARE PRODUCT for any illegal purpose or conduct.

2.2 Back-up. Except as expressly provided for under this Agreement you may not copy the SOFTWARE PRODUCT; except, however, you may keep one copy of the SOFTWARE PRODUCT and, if applicable, one copy of any previous version, for back-up purposes, only to be used in the event of failure of the original. All copies of the SOFTWARE PRODUCT must be marked with the proprietary notices provided on the original SOFTWARE PRODUCT. You may not reproduce the supporting documentation accompanying the SOFTWARE PRODUCT.

2.3 No Modifications. You may not modify, translate or create derivative works of the SOFTWARE PRODUCT.

2.4 Proprietary Notices. You may not remove or obscure any proprietary notices, identification, label or trademarks on or in the SOFTWARE PRODUCT or the supporting documentation.

2.5 Software Transfer. You may permanently transfer all of your rights under this Agreement in connection with transfer of the PRODUCT, provided you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this Agreement, and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade, any transfer must include all prior versions of the SOFTWARE PRODUCT. However, if the SOFTWARE PRODUCT is marked "Not for Resale" or "NFR", you may not resell it or otherwise transfer it for value.

2.6 Copyright. All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and “applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by POLYCOM or its suppliers. Title, ownership rights, and intellectual property rights in the SOFTWARE PRODUCT shall remain in POLYCOM or its suppliers. Title and related rights in the content accessed through the SOFTWARE PRODUCT is the property of such content owner and may be protected by applicable law. This Agreement gives you no rights in such content.

2.7 Confidentiality. The SOFTWARE PRODUCT contains valuable proprietary information and trade secrets of POLYCOM and its suppliers that remains the property of POLYCOM. You shall protect the confidentiality of, and avoid disclosure and unauthorized use of, the SOFTWARE PRODUCT.

2.8 Dual-Media Software. You may receive the SOFTWARE PRODUCT in more than one medium. Regardless of the type or size of medium you receive, you may use only one medium that is appropriate for your single PRODUCT. You may not use or install the other medium on another PRODUCT.

2.9 Reservation of Rights. POLYCOM reserves all rights in the SOFTWARE PRODUCT not expressly granted to you in this Agreement.

2.10 Additional Obligations. You are responsible for all equipment and any third party fees (such as carrier charges, internet fees, or provider or airtime charges) necessary to access the SOFTWARE PRODUCT.

3. SUPPORT SERVICES. POLYCOM may provide you with support services related to the SOFTWARE PRODUCT (“SUPPORT SERVICES “). Use of SUPPORT SERVICES is governed by the POLYCOM policies and programs described in the POLYCOM-provided materials. Any supplemental software code provided to you as part of the SUPPORT SERVICES is considered part of the SOFTWARE PRODUCT and is subject to the terms and conditions of this Agreement. With respect to technical information you provide to POLYCOM as part of the SUPPORT SERVICES, POLYCOM may use such information for its business purposes, including for product support and development. POLYCOM will not utilize such technical information in a form that personally identifies you.

4. TERMINATION. Without prejudice to any other rights, POLYCOM may terminate this Agreement if you fail to comply with any of the terms and conditions of this Agreement. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts. You may terminate this Agreement at any time by destroying the SOFTWARE PRODUCT and all of its component parts. Termination of this Agreement shall not prevent POLYCOM from claiming any further damages. If you do not comply with any of the above restrictions, this license will terminate and you will be liable to POLYCOM for damages or losses caused by your non-compliance. The waiver by POLYCOM of a specific breach or default shall not constitute the waiver of any subsequent breach or default.

5. UPGRADES. If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use the software identified by POLYCOM as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the software that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded SOFTWARE PRODUCT only in accordance with the terms of this Agreement. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single SOFTWARE PRODUCT package and may not be separated for use on more than one PRODUCT.

6. WARRANTY AND WARRANTY EXCLUSIONS.

6.1 Limited Warranty. POLYCOM warrants that (a) the SOFTWARE PRODUCT will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of receipt by you, and (b) any SUPPORT SERVICES provided by POLYCOM shall be substantially as described in applicable written materials provided to you by POLYCOM. POLYCOM does not warrant that your use of the SOFTWARE PRODUCT will be uninterrupted or error free, or that all defects in the SOFTWARE PRODUCT will be corrected. You assume full responsibility for the selection of the SOFTWARE PRODUCT to achieve your intended results and for the installation, use and results obtained from the SOFTWARE PRODUCT. POLYCOM's sole obligation under this express warranty shall be, at POLYCOM's option and expense,

to refund the purchase price paid by you for any defective software product which is returned to POLYCOM with a copy of your receipt, or to replace any defective media with software which substantially conforms to applicable POLYCOM published specifications. Any replacement SOFTWARE PRODUCT will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

6.2 Warranties Exclusive. IF THE SOFTWARE PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, YOUR SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT POLYCOM'S SOLE OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, AND NON-INFRINGEMENT, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. POLYCOM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF THE SOFTWARE PRODUCT. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM POLYCOM OR THROUGH OR FROM THE SOFTWARE PRODUCT SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT.

POLYCOM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT OR MALFUNCTION IN THE SOFTWARE PRODUCT DOES NOT EXIST OR WAS CAUSED BY YOUR OR ANY THIRD PARTY'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO MODIFY THE PRODUCT, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, POWER CUTS OR OUTAGES, OTHER HAZARDS, OR ACTS OF GOD.

7. LIMITATION OF LIABILITY. YOUR USE OF THE SOFTWARE PRODUCT IS AT YOUR SOLE RISK. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF THE SOFTWARE PRODUCT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL POLYCOM OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF POLYCOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, POLYCOM'S ENTIRE LIABILITY SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE PRODUCT OR U.S. $5.00. PROVIDED, HOWEVER, IF YOU HAVE ENTERED INTO A POLYCOM SUPPORT SERVICES AGREEMENT, POLYCOM'S ENTIRE LIABILITY REGARDING SUPPORT SERVICES SHALL BE GOVERNED BY THE TERMS OF THAT AGREEMENT.

8. INDEMNITY. You agree to indemnify and hold harmless POLYCOM and its subsidiaries, affiliates, officers, agents, co-branders, customers or other partners, and employees, from any loss, claim or demand, including reasonable attorneys' fees, made by any third party due to or arising out of your use of the SOFTWARE PRODUCT, your connection to the SOFTWARE PRODUCT, or your violation of the Terms.

9. DISCLAIMER. Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers, or the limitation of liability for personal injury, so the above limitations and exclusions may be limited in their application to you. When the implied warranties are not allowed to be excluded in their entirety due to local law, they will be limited to the duration of the applicable warranty.

10. EXPORT CONTROLS. The SOFTWARE PRODUCT may not be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iraq, Libya, North Korea, Yugoslavia, Iran, Syria, Republic of Serbia, or any other country to which the U.S. has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. By downloading or using the SOFTWARE PRODUCT, you are agreeing to the foregoing and you are representing and warranting

that you are not located in, under the control of, or a national or resident of any such country or on any such list. If you obtained this SOFTWARE PRODUCT outside of the United States, you are also agreeing that you will not export or re-export it in violation of the laws of the country in which it was obtained.

11. MISCELLANEOUS.

11.1 Governing Law. THIS AGREEMENT SHALL BE GOVERNED BY THE LAWS OF THE STATE OF CALIFORNIA AS SUCH LAWS ARE APPLIED TO AGREEMENTS ENTERED INTO AND TO BE PERFORMED ENTIRELY WITHIN CALIFORNIA BETWEEN CALIFORNIA RESIDENTS, AND BY THE LAWS OF THE UNITED STATES. The United Nations Convention on Contracts for the International Sale of Goods (1980) is hereby excluded in its entirety from application to this Agreement.

11.2 Entire Agreement. This Agreement represents the complete agreement concerning the SOFTWARE PRODUCT and may be amended only by a writing executed by both parties. If any provision of this Agreement is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

11.3 Contact. If you have any questions concerning this Agreement, or if you desire to contact POLYCOM for any reason, please contact the POLYCOM office serving your country.

11.4 U.S. Government Restricted Rights. The SOFTWARE PRODUCT and documentation are provided with RESTRICTED RIGHTS. The SOFTWARE PRODUCT programs and documentation are deemed to be “commercial computer software” and “commercial computer software documentation”, respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the SOFTWARE PRODUCT programs and/or documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be “technical data-commercial items” pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

BY INSTALLING, COPYING, OR OTHERWISE USING THIS SOFTWARE PRODUCT YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS INDICATED ABOVE.

4750 Willow Road
Pleasanton, CA 94588
U.S.A.

Software included in this product contains a module called PsyVoIP which is protected by copyright and by European, US and other patents and is provided under licence from Psytechnics Limited.

Portions of this product also include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE:

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).
Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that

distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS