RELEASE NOTES

14.8.6 I December 2017 I 3725-78311-001L

Polycom® Video Border Proxy (VBP™) 7301

Release Notes
Polycom VBP Release
Version 14
Current Version: 14.8.6
Release Date: 12/15/2017

Polycom VBP Release Notes

This document describes the enhancements and fixes for Polycom® Video Border Proxy (VBP®) 7301 software release 14.8.6.

Contents

Revision History

Revision	Date
Release 14.8.6	December 15, 2017
Release 14.8.5	October 30, 2017
Release 14.8.2	April 30, 2017

Supported Platforms

EdgeProtect Platform	Supported Model Number(s)
7000 Series	7300

Supported Endpoints

VBP Release 14.8.6 supports 1,000 registered/provisioned devices, 100 max concurrent traversal calls on the 7301 platform. For registration and calling, the system is expected to function properly with any standards-based H.323 or SIP endpoint and has been successfully tested with the following endpoints.

Endpoint	Supported Version
Polycom Debut	1.2.1
Polycom HDX	3.1.11
Polycom Trio w/Visual+	5.4.2.5400
RealPresence Group Series	6.0.1-340040
RealPresence Desktop	3.7.0.64517 **Note:** Use with the VBP Access Server embedded provisioning feature requires RealPresence Desktop license to be purchased from Polycom. Contact your Polycom sales representative for licensing options.
RealPresence Mobile	3.7 **Note:** Use with the VBP Access Server embedded provisioning feature does not require RealPresence Mobile license purchase from Polycom.
RMX Virtual Edition and RMX1800	8.6.3
RMX2000 (MPMx)	8.5.11.26

Release Notes for the Current Release

VBP 7301 Release 14.8.6

Release Date: December 15, 2017

Security Updates

- SWEET32: 64-bit block cipher vulnerability [EM-18986]
- Insecure TLSv1.0 vulnerability [EM-19286]

SWEET32: 64-bit block cipher vulnerability

SWEET32 vulnerability is addressed in the OpenSSL 1.0.1u patch. The SWEET32 is a vulnerability that affects remote hosts that uses legacy 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability via a Birthday attack, allowing disclosure and possibly hijacking of an authenticated session.

Resolution:

OpenSSL removed triple-DES ciphers from the 'HIGH' keyword and put them into 'MEDIUM' for 1.0.2 and 1.0.1 branches. This mitigates the SWEET32 birthday attack on 64-bit block ciphers.

Insecure TLSv1.0 vulnerability

The BOA is configured to support TLS version selection. Without this option, the SSL/TLS server supports TLSv1.0, an insecure protocol. The TLSv1.0 encryption uses either RC4 stream cipher or block cipher which are known to have biases and POODLE attack vulnerability.

Resolution:

TLS protocol version is configurable for BOA. This enables the user to configure BOA to select preferred TLS version.

What's New in Release 14.8.6

The following feature is new in this release:

- Access Proxy/Server configured to choose TLS version and cipher

Access Proxy / Server configured to choose TLS version and cipher

Feature No: EM-19334

TLS protocol version and the cipher is configurable in Access Proxy/Server. Without this option, the SSL/TLS server supports TLSv1.0 which is an insecure and obsolete protocol.

Issues Resolved in Release 14.8.6

Issue No.	Case No.	Description	Component
EM-19415	—	Even after configuring the Access Server to TLSv1.2 the Access Server responds with TLSv1.0	Access Server
EM-19426	—	CLI upgrade does not create .netrc files automatically. For FTP upgrades, .netrc files should be created automatically	Upgrade

Known Issues in Release 14.8.6

There are no known issues in release 14.8.6.

Firmware Upgrade Instructions

You must perform a backup of the currently running configuration before you upgrade to new VOS. If you downgrade, you must restore the saved configuration from the previous VOS version.

Attention

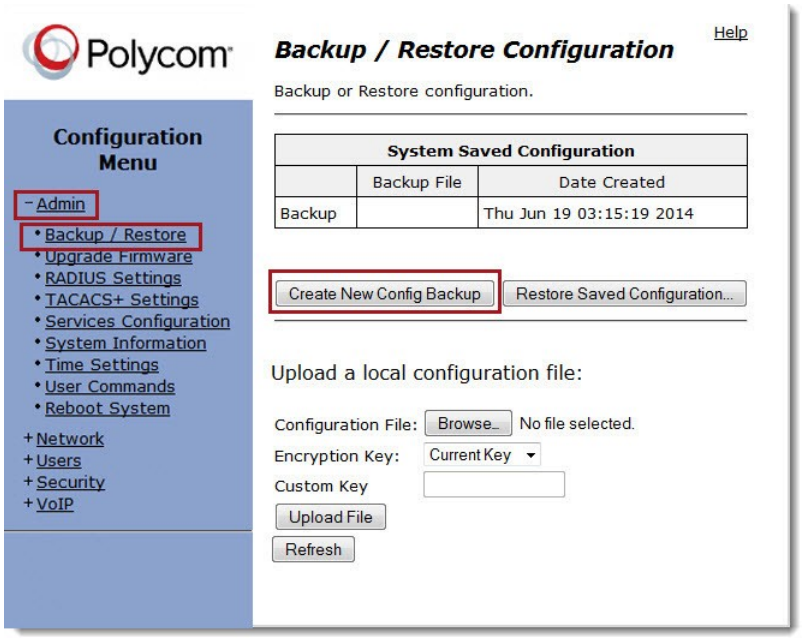
When you update your software, video services will be unavailable for several minutes. It is therefore advised that upgrades be performed during a window when video traffic can be interrupted.

Save Your Configuration

Prior to upgrade, use the VOS Backup / Restore option to save the currently running configuration and store it offline as follows:

1. Open the VBP 7301 user interface in a browser.
2. Choose **Admin > Backup / Restore** from the Configuration Menu. The Backup / Restore Configuration page displays (Figure 1).

Figure 1 Backup / Restore Configuration



3. Click **Create New Config Backup**.

   A pop up box displays to alert you that you will be overwriting a previously saved configuration.

4. Click **OK** in the pop up box. The file name appears in the Backup File column.
5. Click on the filename to prompt the system to download a copy of the backup file and save the file to your local drive.
6. Reboot your system as described in Reboot Your System.

Reboot Your System

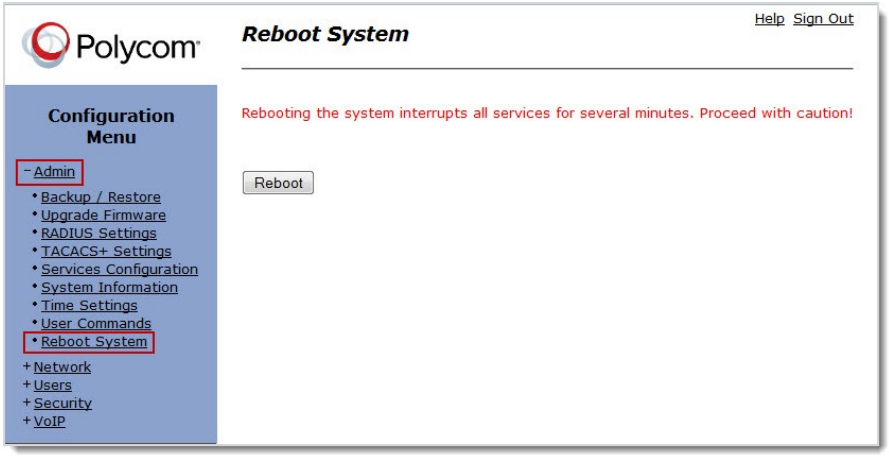
Reboot the VBP 7301 prior to doing the upgrade to be sure there is enough dynamic memory available to handle the upgrade process.

Caution

Rebooting the system interrupts all services for several minutes.

1. Choose **Admin** > **Reboot System** from the Configuration Menu (Figure 2).

Figure 2 Reboot System



2. Click **Reboot**.

   The following message is displayed:

   WARNING: All voice, video, and data services will be interrupted. They will be unavailable for several minutes while the system reboots. Do you want to continue?

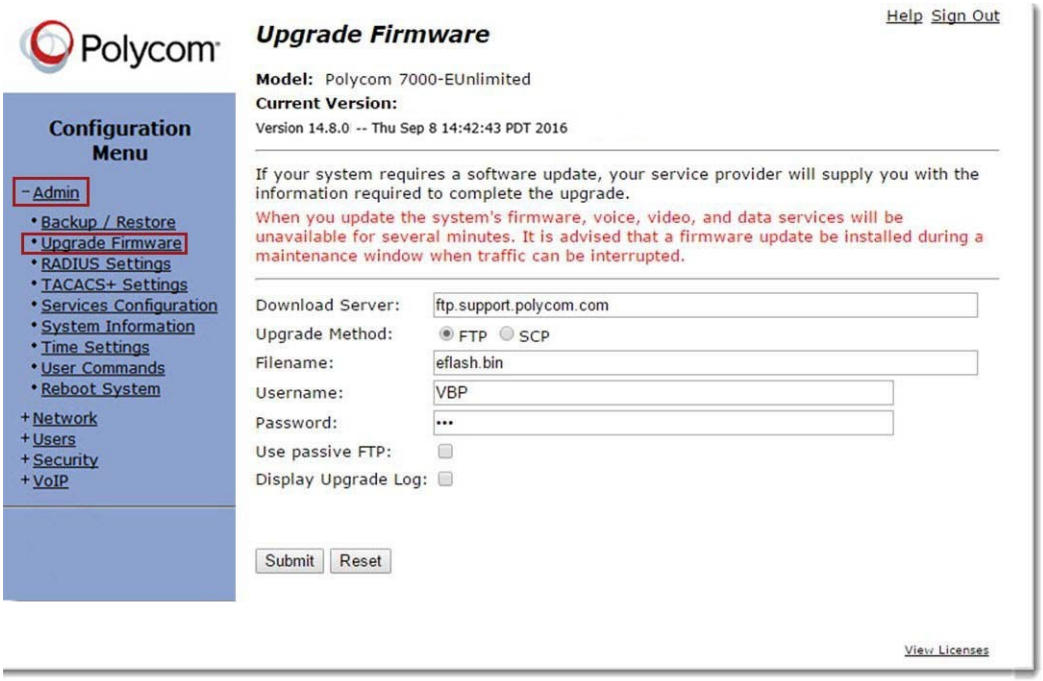
3. Click **OK** to continue.
4. Allow several minutes for the reboot to complete.
5. Upgrade your firmware as described in Upgrade Your Firmware.

Upgrade Your Firmware

After saving your old configuration and rebooting your system, upgrade to new firmware as follows:

1. Log back in to the VBP 7301.
2. Choose **Admin** > **Upgrade Firmware** from the Configuration Menu (Figure 3).

Figure 3 Upgrade Firmware



3. Enter the firmware upgrade information:
   a. Enter the Download server: **ftp.support.polycom.com**
   b. Select the Upgrade Method: **FTP**
   c. Enter the filename: **eflash.bin**
   d. Enter the Username: **VBP**
   e. Enter the password: **VBP**

Note

If upgrading from Version 14.0.1, enter the following:

Username: **plcm**
Password: **plcm123**

4. Click **Submit**.

Restoring or Downgrading Your Configuration

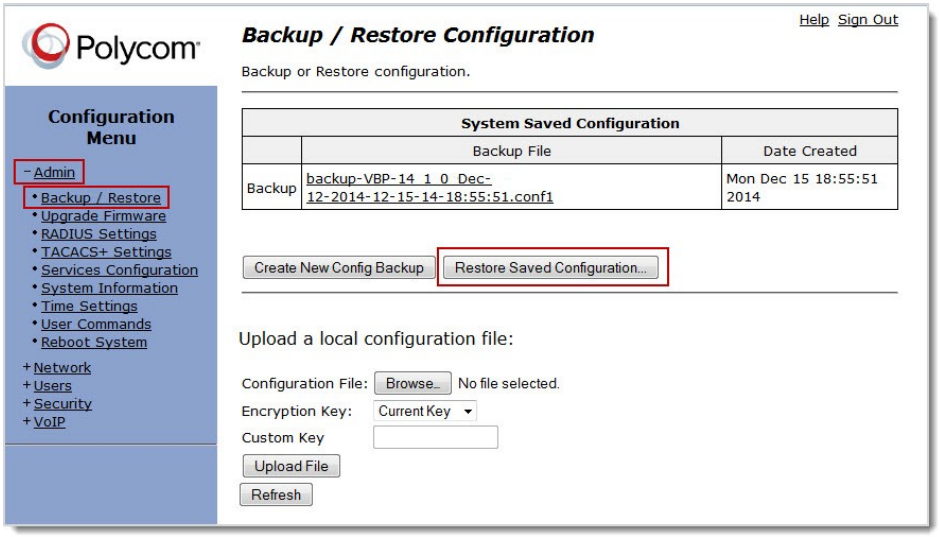
If for any reason you need to downgrade to the previous firmware version, you must first downgrade the VOS version and then restore the saved configuration using the Backup / Restore Configuration page. Your firmware is downgraded to the version that was running on the system before the downgrade procedure.

Note

It is strongly recommended that you restore the same firmware version that was previously configured on your system.

1. Choose **Admin** > **Backup / Restore** from the Configuration Menu (Figure 4).

Figure 4 Restore Saved Configuration



2. Click **Browse** and select the saved configuration file from your desktop. Click **Upload File**. The backup file appears in the Backup File column.

3. To restore to a previously saved configuration, click **Restore Saved Configuration**.

Obtaining Further Assistance

For more information about installing, configuring, and administering Polycom products, refer to Documents and Downloads at Polycom Support.

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

North America:
Tel: +1 408 5866000
Tel: +1 800 7659266

Sales: 1.800. POLYCOM, or 408.526.9000

Release Notes for the Previous Release

VBP 7301 Release 14.8.5

Release Date: October 30, 2017

Security Updates

- Cross-Site Request Forgery and Clickjacking vulnerability [EM-18010]
- Anti-clickjacking Frame Header Vulnerability [EM-16258]

Cross-Site Request Forgery and Clickjacking vulnerability

Anti-forgery tokens or request verification tokens are added to web forms to verify intent. The anti-CSRF tokens will prevent any attack that forces unauthorized command transmissions from a user trusted by web applications.

X-Frame-Options: DENY header included in HTTP responses will mitigate the clickjacking vulnerability. Clickjacking will compromise sensitive information and weaken the effectiveness of a user's system security configuration.

Resolution

Anti-CSRF tokens are inserted in HTML Forms. They are validated on POST requests before saving submitted changes.

X-Frame-Options: DENY headers are sent in HTTP responses. Earlier, the X-Frame-Options response header was only sent in HTTPS responses.

Anti-clickjacking Frame Header Vulnerability

X-Frame-Options: DENY header is now included in HTTP responses to mitigate the anti-clickjacking frame header vulnerability. Exploitation of this vulnerability may allow a remote attacker to obtain sensitive information, hijack users' click and even alter a user's system security configuration.

Resolution

X-Frame-Options: DENY headers are sent in HTTP responses. Earlier, the X-Frame-Options response header was only sent in HTTPS responses.

Issues Resolved in Release 14.8.5

Issue No.	Case No.	Description	Component
EP-1185	57592	B2BUA video calls placed between a pair of HA Edgeprotect ESBCs result in one-way media	Access Proxy, B2BUA, HA
EP-1199	61341	Registration issue during new client registration as ST box responds with an RRJ or “e_fullRegistrationRequired” message	H323
EM-16571	—	In WAN2WAN calls,PLCM endpoint cannot send content until it receives content	H323

Known Issues in Release 14.8.5

There are no known issues in 14.8.5.

VBP 7301 Release 14.8.2

Release Date: January 30, 2017

Security Updates

OpenSSH Vulnerability [EM-14607]

OpenSSH version 7.2p2 has been released to address a vulnerability in all prior versions. Exploitation of this vulnerability may allow a remote attacker to obtain sensitive information.

VBP 7301 uses openssh-6.1p1 version, which is vulnerable to attack.

Affected configurations: All versions of OpenSSH prior to 7.2p2 with X11Forwarding enabled.

Resolution

Set X11Forwarding=no in sshd_config. This is the default.

OpenVPN Denial of Service Vulnerability [EM-14352]

CVE-2015-3193

CVE-2015-3194

CVE-2015-3195

CVE-2015-3196

CVE-2015-1794

Description

OpenSSL has released updates patching four vulnerabilities. Exploitation of one of these vulnerabilities could allow an attacker to cause a denial-of-service condition. Updates available include:

- OpenSSL 1.0.2e for 1.0.2 users
- OpenSSL 1.0.1q for 1.0.1 users
- OpenSSL 1.0.0t for 1.0.0 users
- OpenSSL 0.9.8zh for 0.9.8 users

Resolution

OpenSSL 1.0.2 users should upgrade to 1.0.2e.

What's New in Release 14.8.2

The following features are new in this release:

- Access Server Bandwidth Provisioning
- Polycom Endpoints Added to Access Server Provisioning
- PPPoE Support on the VBP 7301
- SIP - LAN/WAN Side Refresh Interval
- SIP URI Available on the Access Server GUI
- VoIP Configuration Page Support

Access Server Bandwidth Provisioning

Feature No: EP-1178

Access Server can now provision bandwidth limits separately for LAN and WAN.

Polycom Endpoints Added to Access Server Provisioning

Feature No: EM-16829

Polycom RealPresence Debut has been added as an endpoint type in Access Server provisioning.

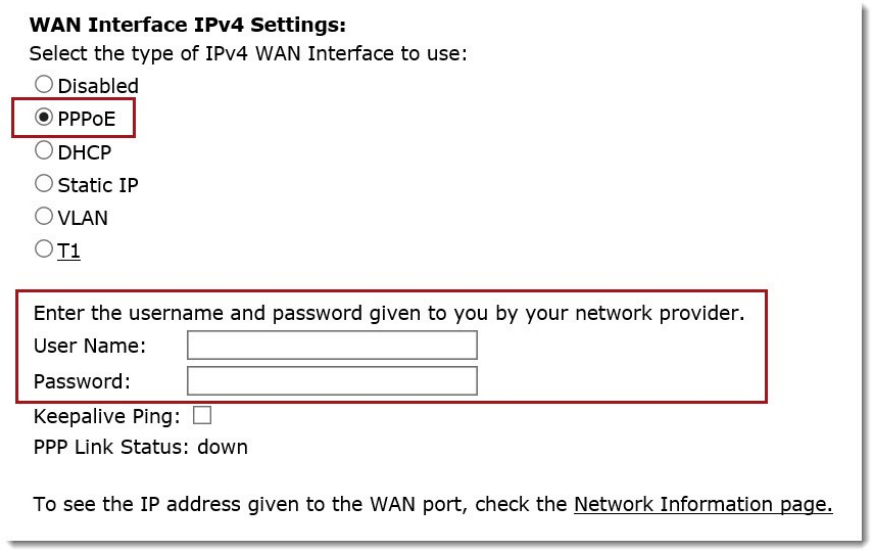
PPPoE Support on the VBP 7301

Feature No: EM-14754

The VBP 7301 now supports PPP sessions over the WAN Ethernet port. To enable the feature:

1. Choose Network from the Configuration Menu.
2. Scroll to **WAN Interface IPv4 Settings** and select the **PPPoE** radio button (Figure 5).

Figure 5 Network Configuration Page - IPv4 PPPoE Settings



3. Enter the PPPoE username and password given by your ISP in the fields provided and click **Submit**.

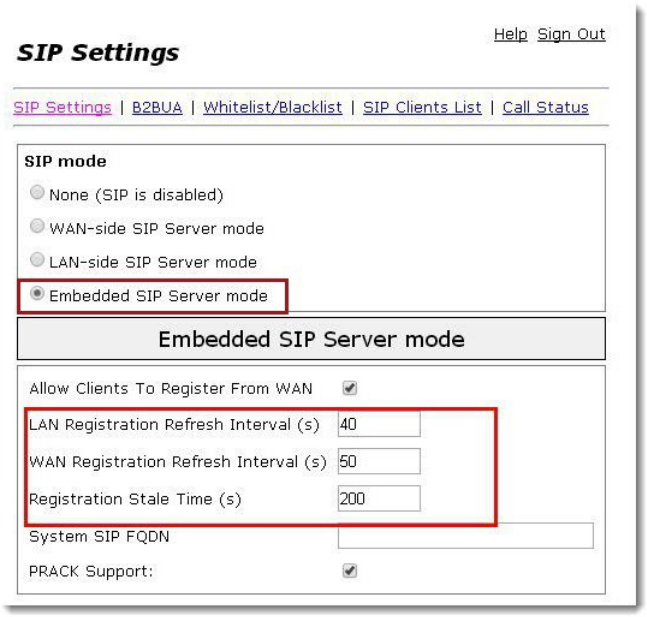
SIP - LAN/WAN Side Refresh Interval

Feature No: EP-1096

In Embedded SIP Server Mode, this allows for configuring separate registration refresh intervals for LAN and WAN side clients.

1. Choose **VoIP** > **SIP** > **SIP Settings** (Figure 6).
2. Select the **Embedded SIP Server Mode** radio button.

Figure 6 SIP Settings Configuration Page



3. Configure the following Embedded SIP Server mode settings:
   - **LAN Registration Refresh Interval**— The system configures this as the Expires value in the 200 OK message to a client in response to a successful registration. Default value: 300
   - **WAN Registration Refresh Interval**— The system configures this as the Expires value in the 200 OK message to a client in response to a successful registration. The WAN Registration Refresh Interval is more frequent than the corresponding LAN Interval in order to maintain registration status across NAT devices. Default value: 45
   - **Registration Stale Time**— Defines the time a client entry is valid on the system. Each WAN or LAN side endpoint has a system client list entry with activity timers to determine if the client is actively sending keepalive registration messages. When a WAN or LAN side client fails to update its registration entry on the system with the time specified in this field, the system will remove the client from the SIP clients list. Default range is 2 times the registration refresh interval to 9999.

     Example: When the registration refresh timer is set to 45, the range for the registration stale time is 90-9999.

4. Click **Submit** to save your changes.

SIP URI Available on the Access Server GUI

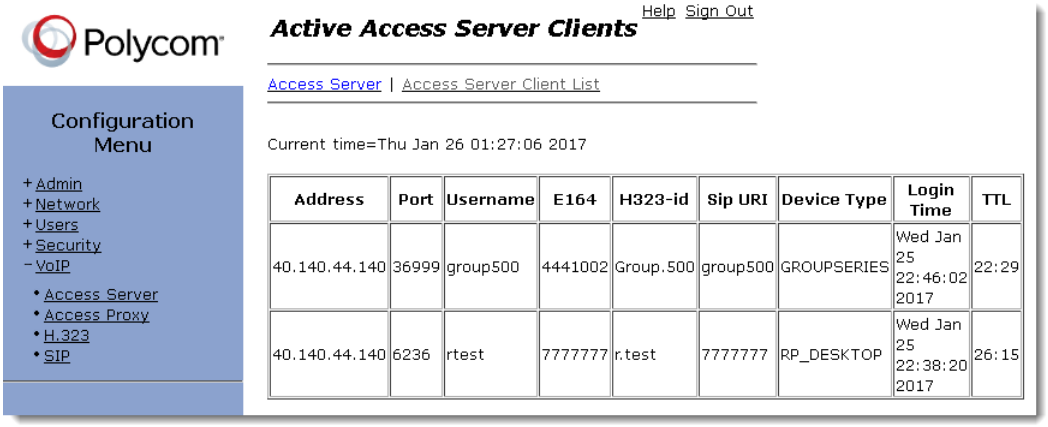
Improvement No: EM-16522

The current Access Server/Access Proxy Clients List display shows only H.323-related

alias values (e164 and H323-ID). Release 14.8.2 adds SIP URI to the display. Sign in to the Access Server with a supported Polycom video endpoint (GS, HDX, RPM, RPD, Debut) and on an account that has SIP enabled, the Access

Server Clients endpoint entry in the list will also now have the SIP URI listed in addition to H.323 alias values (Figure 7).

Figure 7 Access Server Page

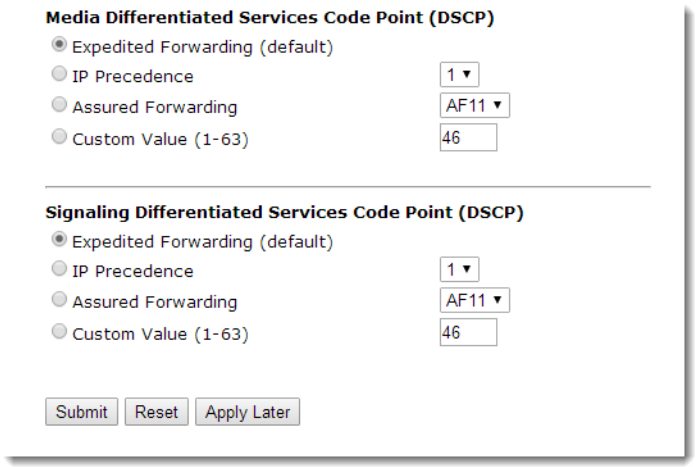


VoIP Configuration Page Support

Feature No: EM-15842

Media Differentiated Services Code Point (DSCP) and Signaling Differentiated Services Code Point (DSCP) options are now displayed on the VBP 7301 VoIP page. You can now change the signaling or media markings settings using these fields on the page (Figure 8).

Figure 8 VoIP Configuration - DSCP Settings



Issues Resolved in Release 14.8.2

Issue No.	Case No.	Release Note	Component
EM-15272	—	Added syslog messaging for Access Server authentication events.	Access Server
EP-923	48150	Reduced the number of items in Access Server provisioning to allow for local control of settings that are not necessarily common to all devices	Access Server
EM-16108	—	Corrected an issue in the SIP messaging timeout code that caused ALG to exit.	ALG
EM-15048	—	Polycom proprietary SVC headers are no longer stripped from the Invite by B2BUA.	B2BUA
EM-15381	—	B2BUA strips contact header in 200OK response to re-invite.	B2BUA
EM-14922	52238	SIP embedded mode SIP TLS endpoint is dialing B2B TLS, call leaves WAN on TCP5060.	B2BUA
EM-15762	—	The Call Terminate icon is not shown on the call list when making a LAN to LAN call in GK-Routed mode.	H.323
EM-15467	—	Added syslogs for licensed call count exceeded, and to indicate when call count is being incremented or decremented.	H.323
EP-961	—	Support for Inside/Outside TLS mode, contact your Polycom system engineer for more information.	H.323
EP-628	—	In peering proxy mode, routing a call using the default address fails if no destination alias is specified by the caller.	H.323
EM-16383	—	VBP 7301 receives SIP UPDATE request via TCP, then sends to TCP registered client via UDP causing the call to drop.	Local Call Control SIP
EM-15172 EM-1140 escviu-214	—	Implement automatic re-issue of invite upon receipt of 416 in SIP TLS for HDX — Send SIP with transport=TLS instead of sips in invite header.	None
EM-16204	53509	Network Time Protocol configuration fields do not accept IPv6 addresses.	NTP
EM-16358	53560	Added support for DigiCert as a root CA.	Security
EM-15182	—	Intrusion Prevention events are sent to SYSLOG.	Security
EP-1049	—	On the **Security** > **HTTPS Configuration** page, clearing the Alternate HTTPS port field should reset it to the default value 8443 not 443.	Security
EP-1154	52982	SIP calls to the cloud service do not connect due to incorrect transport in ACK from the VBP 7301.	SIP
EP-846	—	When in LAN/WAN side SIP server mode, the SIP server becomes unreachable when SIP transport is set to TLS.	SIP

Issue No.	Case No.	Release Note	Component
EP-1103	—	Embedded SIP server: A delay observed when registering the SIP client.	SIP
EM-15325	—	Entering an IPv6 address in the SIP Server Address field returns an IP address invalid error.	SIP
EM-16222	—	On the SIP Settings page, the TLS Protocol now uses Javascript to auto-populate the ciphers string based on TLS protocol version selected.	SIP (VBP)
EM-16157	—	SIP calls to the cloud result in signaling loop when 302 response is received.	SIP Video
EM-16221	—	All ciphers related to SSLv3 protocol are now disabled.	TLS for SIP
EM-15361	—	Static Routes page: add text indicating the maximum amount of static routes that can be configured.	UI

Known Issues in Release 14.8.2

There are no known issues in this release.

Legal Information

Copyright

Trademarks

EDGEWATER NETWORKS and Design, EDGEMARC, EdgeMarc, and EDGECONNECT are registered trademarks of Edgewater Networks, Inc. EDGEWATER NETWORKS and EDGEVIEW are trademarks of Edgewater Networks, Inc. Any other trademarks appearing in this manual are owned by their respective companies.

Copyright

Export Notice

You (Purchaser) acknowledge that these products are subject to the U.S. Export Administration Regulations (the “EAR”) and that you will comply with the EAR. You are not located in Cuba, Iran, North Korea, Sudan, or Syria. You will not export or re-export this product, directly or indirectly, to: (1) any countries that are subject to US export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan, or Syria);(2)any end user who you know or have reason to know will utilize them in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, and sounding rockets, or unmanned air vehicle systems; or (3) any end user who has been prohibited from participating in US export transactions by any federal agency of the US government. In addition, you are responsible for complying with any local laws in your jurisdiction which may impact your right to import, export or use these products.

Licensing

Use of this product is subject to Edgewater Networks Software License Agreement. Portions of this product include software sponsored by the Free Software Foundation and are covered by the GNU GENERAL PUBLIC LICENSE.

Refer to www.edgewaternetworks.com/licensing for more information regarding licenses and the warranty.

Typographical Errors

This publication could include technical inaccuracies or typographical errors, for which Edgewater Networks never can or shall be held liable. Changes are made periodically to the information herein; these changes will be incorporated in new releases of this publication. Edgewater Networks may make improvements or changes in the product or products described in this publication at any time, without prior notice.