



RELEASE NOTES

14.8.2 | January 2017 | 3725-78311-0011

Polycom[®] Video Border Proxy (VBP[™]) 7301



Polycom VBP Release Notes

This document describes the enhancements and fixes for Polycom® Video Border Proxy (VBP™) 7301 software release 14.8.2.

Contents

Revision History	1
Supported Platforms	2
Supported Endpoints	2
Release Notes for the Current Release	3
VBP 7301 Release 14.8.2	3
What's New in Release 14.8.2	4
Issues Resolved in Release 14.8.2	8
Known Issues in Release 14.8.2	9
Firmware Upgrade Instructions	9
Save Your Configuration	9
Reboot Your System	10
Upgrade Your Firmware	11
Restoring or Downgrading Your Configuration	13
Obtaining Further Assistance	14
Copyright and Trademark Information	7

Revision History

Revision	Date
Release 14.8.2	01/30/2017

Supported Platforms

VBP Platform	Supported Model Number(s)
7000 Series	7301

Supported Endpoints

VBP 7301 Release 14.8.2 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 14.8.2

Release Date: January 30, 2017

Security Updates

- [OpenSSH Vulnerability \[EM-14607\]](#)
- [OpenVPN Denial of Service Vulnerability \[EM-14352\]](#)

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 1).

Figure 1 Network Configuration Page - IPv4 PPPoE Settings

WAN Interface IPv4 Settings:
Select the type of IPv4 WAN Interface to use:

Disabled
 PPPoE
 DHCP
 Static IP
 VLAN
 T1

Enter the username and password given to you by your network provider.
User Name:
Password:

Keepalive Ping:
PPP Link Status: down

To see the IP address given to the WAN port, check the [Network Information page](#).

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 2).
2. Select the **Embedded SIP Server Mode** radio button.

Figure 2 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 3).

Figure 3 Access Server Page

Active Access Server Clients [Help](#) [Sign Out](#)

[Access Server](#) | [Access Server Client List](#)

Current time=Thu Jan 26 01:27:06 2017

Address	Port	Username	E164	H323-id	Sip URI	Device Type	Login Time	TTL
40.140.44.140	36999	group500	4441002	Group.500	group500	GROUPSERIES	Wed Jan 25 22:46:02 2017	22:29
40.140.44.140	6236	rtest	7777777	r.test	7777777	RP_DESKTOP	Wed Jan 25 22:38:20 2017	26:15

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 4).

Figure 4 VoIP Configuration - DSCP Settings

Media Differentiated Services Code Point (DSCP)

- Expedited Forwarding (default)
- IP Precedence
- Assured Forwarding
- Custom Value (1-63)

Signaling Differentiated Services Code Point (DSCP)

- Expedited Forwarding (default)
- IP Precedence
- Assured Forwarding
- Custom Value (1-63)

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

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.

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 5](#)).

Figure 5 Backup / Restore Configuration

Polycom **Backup / Restore Configuration** [Help](#)

Backup or Restore configuration.

Configuration Menu

- Admin
- Backup / Restore
- Upgrade Firmware
- RADIUS Settings
- TACACS+ Settings
- Services Configuration
- System Information
- Time Settings
- User Commands
- Reboot System
- + Network
- + Users
- + Security
- + VoIP

System Saved Configuration

	Backup File	Date Created
Backup		Thu Jun 19 03:15:19 2014

Upload a local configuration file:

Configuration File: No file selected.

Encryption Key: ▾

Custom Key

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 file name 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.

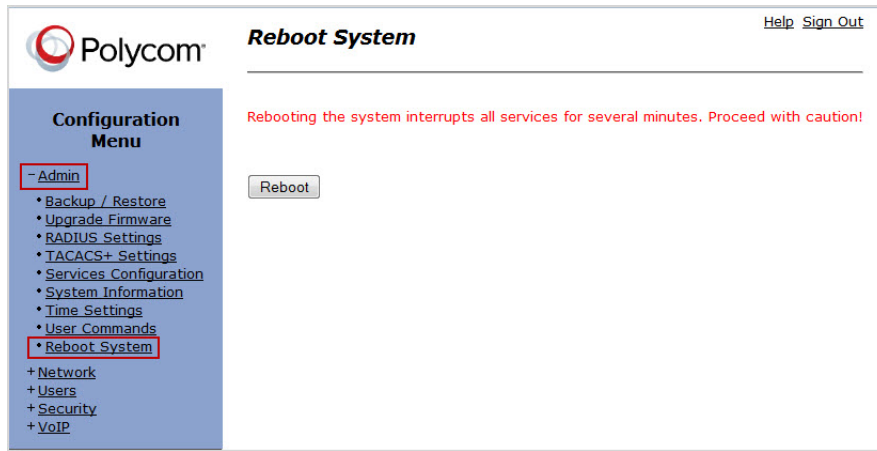


Caution

Rebooting the system interrupts all services for several minutes.

1. Choose **Admin > Reboot System** from the Configuration Menu ([Figure 6](#)).

Figure 6 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 7](#)).

Figure 7 Upgrade Firmware

Polycom **Upgrade Firmware** [Help](#) [Sign Out](#)

Model: Polycom 7000-EUnlimited
Current Version:
 Version 14.8.0 -- Thu Sep 8 14:42:43 PDT 2016

If your system requires a software update, your service provider will supply you with the information required to complete the upgrade.
 When you update the system's firmware, voice, video, and data services will be unavailable for several minutes. It is advised that a firmware update be installed during a maintenance window when traffic can be interrupted.

Download Server:
 Upgrade Method: FTP SCP
 Filename:
 Username:
 Password:
 Use passive FTP:
 Display Upgrade Log:

[View Licenses](#)

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 8).

Figure 8 Restore Saved Configuration

Backup / Restore Configuration [Help](#) [Sign Out](#)

Backup or Restore configuration.

System Saved Configuration		
	Backup File	Date Created
Backup	backup-VBP-14_1_0_Dec-12-2014-12-15-14-18:55:51.conf1	Mon Dec 15 18:55:51 2014

Upload a local configuration file:

Configuration File: No file selected.

Encryption Key: ▾

Custom Key

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

Copyright and Trademark Information

Copyright© 2017, Polycom, Inc. All rights reserved. No part of this document may be reproduced, translated into another language or format, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Polycom, Inc.

6001 America Center Drive
San Jose, CA 95002
USA

Trademarks Polycom®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries.



All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

End User License Agreement By installing, copying, or otherwise using this product, you acknowledge that you have read, understand and agree to be bound by the terms and conditions of the End User License Agreement for this product. The EULA for this product is available on the Polycom Support page for the product.

Patent Information The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.

Open Source Software Used in this Product This product may contain open source software. You may receive the open source software from Polycom up to three (3) years after the distribution date of the applicable product or software at a charge not greater than the cost to Polycom of shipping or distributing the software to you. To receive software information, as well as the open source software code used in this product, contact Polycom by email at OpenSourceVideo@polycom.com.

Disclaimer While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.

Polycom Support Visit the [Polycom Support Center](#) for End User License Agreements, software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.