

Patch Release Notes



Polycom® RealPresence® Distributed Media Application™

Release label:	6.4.1_P4	(6.4.1_P4_Build_238776-full.bin)
Built on versions:	Polycom DMA Systems v6.4.1.1, v6.4.1.2, v6.4.1.3	
Released files:	ISO, OVA, Hyper-V and the upgrade file	

Purpose

DMA v6.4.1.4 replaces both DMA v6.4.1.2 and DMA v6.4.1.3 and for stability reasons. Polycom highly recommends customers on previous releases to upgrade to DMA v6.4.1.4 as soon as possible.

DMA v6.4.1.4 contains all fixes from all previous v6.4.1.x releases. The sections below indicate the Resolved Issues based on the version that they were fixed.

Resolved Issues from DMA v6.4.1.4

Patch 4 for DMA 6.4.1 (i.e. v6.4.1.4 or v6.4.1_P4) has been augmented with the following items:

Key	Summary
DMA-16964	<p>Disabling TLS 1.0 in DMA 6.4.1.2 and 6.4.1.3 could result in the inability of DMA to reboot.</p> <p>If you are using a secured Management connection between the DMA and RMX, the following will apply.</p> <p>If TLSV1 (or another TLS version) is disabled on DMA, you'll need to add a flag to the RMX via RMX Manager to support another TLS or SSL version. From RMX V8.6.7 release notes:</p> <p>1.RMX Manager > Add and connect your MCU > Setup > System Config > System Config > MCMS_PARAMETERS_USER > New Flag.</p> <p>2.Flag Name = RMX_MANAGEMENT_SECURITY_PROTOCOL. Flag value = the default value is TLSV1_SSLV3 so you'll need to alter that to fit whichever protocol you are using. Setting it to TLS1_2_TLSV1_1_TLSV1 will cover all three TLS versions regardless of which are enabled (you need at least one TLS version enabled).</p> <p>After setting to TLS1_2_TLSV1_1_TLSV1, Apache is able to speak on TLS 1.0, TLS 1.1 and TLS 1.2. After setting to TLSV1_SSLV3, Apache only speaks on TLS 1.0</p> <p>Please refer to the RMX Documentation for further details.</p>
DMA-16943	H323 call leaks are seen on the dashboard and lead to licenses being maxed out
DMA-16939	DMA incorrectly quarantines RPD users

Resolved Issues from DMA v6.4.1.3

Key	Summary
DMA-16896	Inbound calls from an external GK neighbor to a DMA supercluster can potentially fail if the call SETUP happens on a different cluster than where the initial LRQ was received.
DMA-16918	DMA CDRs displaying 'Source' and 'Destination' as same, impacting RPAanalytics system and customer reports
DMA-16935	Change/hide RealConnect Bridge user name in the Skype roster. There is a new setting on the Conference Settings page: "Skype roster cascade indicator". This setting specifies the display name that appears in the Skype-for-business client as the conference roster entry for the Polycom conference (with all the standards-based endpoints). The setting consists of 0-64 characters, consisting of the ascii letters (upper/lower case) + digits (0-9) + (space ! % + - _). If left blank, the value is <conf-ID>@domain, where the conf-ID is the name of the ID of the Polycom conference (e.g., the RealConnect ID or VMR). This improvement works in conjunction with RMX version 8.7.4.x as well as 8.7.5.x and beyond.
DMA-16941	Support for VMWare 6.5 in DMA OVA

Resolved Issues from DMA v6.4.1.2

Key	Summary
DMA-15995	DMA dashboard shows calls that do not reflect on actual calls If an endpoint becomes unreachable, DMA will hold onto the call in hopes that the endpoint recovers. If the endpoint doesn't recover within 2.5 hours, the DMA will tear down the call and release the license.
DMA-16222	DMA performance problems resulting from frequent endpoint re-registration
DMA-16854	Upgrading Hyper-V Fails
DMA-16868	DMA - Site Name on RMX displays with incorrect participant name.
DMA-16869	In certain environments, RealConnect calls may fail if the DMA is unable to open port 443 to the Lync edge server.
DMA-16878	An unusually long running diagnostic statement triggered a missed heartbeat and failover
DMA-16882	DMA 6.4.1 and 6.4.1.1 show "Rejected: Insufficient network bandwidth available" as disconnection cause for successful calls
DMA-16883	An invalid Request URI causing the call to fail when it is sent to the RMX
DMA-16886	Stale calls in Active Calls list cause it to reach the call license limit
DMA-16904	SIP calls are disconnecting every 30 minutes when dialing to WEB EX, all other SIP calls to other external entities do not experience this issue

Known Issues

Issues that have been identified since the release of DMA 6.4.1.1 and are not included in DMA 6.4.1.4 but are aimed to be fixed in a future release.

Key	Summary
DMA-16847	Installation of server certificate on DMA will fail if there are ~15 or more root CA certificates installed
DMA-16849	DMA Shared Number Dialing - Direct Dial will accept resolve true for any IP address.
DMA-16850	Exchange Server integration disabled in v6.4.1
DMA-16852	DMA SNMP settings does not update FW config when changing transport protocol
DMA-16857	DMA 6.4.0.1 does not display unique SNMP engine ID for each DMA node in VIP GUI.
DMA-16880	SIP calls time out before connecting if unrelated SIP peer FQDNs cannot be resolved
DMA-16892	DMA rejects RMX SIP registrations with 500 Server Internal Error, but status OK on RMX no discernible service impact-
DMA-16908	DMA responded to incoming VEQ/VMR calls with 503 Service unavailable.
DMA-16912	Participant status is not reported correctly to RPRM in some cascade-for-size calls
DMA-16920	Garbage Collection pauses resulted in territory failover
DMA-16922	Unable to log in to DMA via web UI using local\admin or AD accounts. Reboot of DMA resolved the issue
DMA-16938	Ghost conference stuck and will not clear via REST API
DMA-16940	DMAs experience occasional performance issues caused by rolling logs at the top of the hour
DMA-16944	Using Passcode and Aliases settings on the DMA when the Conference password parameter is enabled, the password request prompt is been played on H323
DMA-16951	The OrigEndpoint field in CDR has all the Codes of the Immersive System rather than One codec
DMA-16954	Calls with "SERVICE_DOWN" end event are not showing in the GUI CDR export
DMA-16956	CDR call and conf counts are different between GUI vs. API queries
DMA-16960	RealConnect functionality in conjunction with cascade for size, participants connected to slave RMX conference hear IVR waiting for chairperson

© 2017 Polycom, Inc. All rights reserved. POLYCOM®, the Polycom logo, and the names and marks associated with Polycom's 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.

Prerequisites/Configuration Considerations

- Systems may have Polycom DMA v6.1.x, v6.2.x, v6.3.x or previous versions of v6.4.x
- When upgrading from DMA 6.1.x, 6.2.x, 6.3.x or 6.4.x to 6.4.1.3, the system will not preserve the call history information. To keep this data, backup the databases, upgrade the DMAs, and then restore the databases.
- A DMA must be taken out of a Supercluster to perform this upgrade.

Supported Upgrade Paths

Current Version	Intermediate Upgrade	Intermediate Upgrade	Final Upgrade	New License Required?
5.0.x, 5.1.x, 5.2.0	→ 5.2.1 ¹	→ 6.2.2.2 ²	→ 6.4.1.4 ³	Yes.
5.2.1, 5.2.2.x, 6.0.x	→ 6.2.2.2 ²		→ 6.4.1.4 ³	Yes.
6.1.x, 6.2.x			→ 6.4.1.4 ³	Yes.
6.3.x			→ 6.4.1.4 ³	Yes
6.4.x			→ 6.4.1.4 ³	No.
1. Use DMA-upgrade 5.2.1-bld8r112427.bin to upgrade to 5.2.1. 2. Use 6.2.2 P2 Build 202581-rppufconv.bin to upgrade to 6.2.2.2. 3. Use 6.4.1 P4 Build 238776-full.bin to make the final upgrade to version 6.4.1.4.				

Note: 6.2.2.2 was selected because it is the most recent GA release that will allow an upgrade from a pre-6.1.0 system.

Installation Notes

1. It is always recommended that configuration backups are taken before upgrades. Please follow the instructions in the OPERATIONS GUIDE for the Polycom® RealPresence® Distributed Media Application™ (DMA®) System which can be found on the Polycom Support site:
http://support.polycom.com/content/dam/polycom-support/products/UC-Infrastructure-Support/collaboration_conferencing_platforms/user/en/DMA-6-4-0-Operations-Guide.pdf
2. Download the upgrade file for DMA v6.4.1_P4
3. Login to DMA and navigate to Maintenance > Software Upgrade
4. Select "Upload and Upgrade" and choose the upgrade file
5. DMA processes and applies patch
6. NOTE: If you are performing an upgrade on Hyper-V you will observe:
 - a. A warning screen with a green status bar and flashing red text bar.
 - b. When the status bar completes, a flashing red screen will be displayed.

- c. The upgrade should successfully complete several minutes after the flashing red screen is first observed.
- d. A few minutes after you see the flashing red screen, try to open the DMA GUI window.
- e. If it doesn't come up immediately, wait and try again.
- f. It may take up to an hour after the upgrade begins for it to complete, so continue to try to load the DMA GUI window.

Automatically send usage data

DMA will automatically send usage data if you have checked the "Automatically send usage data" checkbox while accepting the End User License Agreement (EULA). To see what you have selected; you can go to Admin->Local Cluster->Licenses on the DMA UI. A description on what type of data is sent is provided in the DMA Operations Guide under section "Automatically Send Usage Data". As this data is used to continually improve the product, Polycom recommends that this be kept enabled.

Please note that if your local DNS server does not resolve `customerusagedatacollection.polycom.com`, the Analytics service in DMA will query to Google DNS server (8.8.8.8) to resolve that DNS name.

To see the actual data being sent to Polycom from DMA, go to Maintenance->System Log Files on the DMA UI. Select a log archive and click on "Download Archived Logs". After the log archive is downloaded on your local machine, unpack the log archive. In the main directory, you will see a file called `analytics.json`. That file contains the data that is being sent.