Patch Release Notes

Polycom® RealPresence® Distributed Media Application™

Release label:	6.4.1_P6	(6.4.1_P6_Build_240027-full.bin)
Built on versions:	Polycom DMA System v6.4.1.5	
Released files:	ISO, OVA, Hyper-V and the upgrade file	

Purpose

DMA v6.4.1.6 contains all fixes from all previous v6.4.1.x releases.
The sections below indicate the Resolved Issues based on the version in which they were fixed.

Note/Warning:
These steps are mandatory prior to upgrading to DMA v6.4.1.6.
Failure to follow these steps may cause the DMA to fail to boot.

A. If upgrading from a DMA version 6.2.x or earlier, it is mandatory to perform Intermediate Upgrades listed in the "Supported Upgrade Paths" table to get to DMA v6.3.2.4.
B. Once the DMA is at or above v6.3.2.4, perform the following before upgrading to DMA v6.4.1.6:
1) Go to Admin -> Local Cluster -> Security Settings
2) Toggle the 'Ignore SIP "critical" privacy flag'
3) Click "Update"
4) **Repeat steps 2 & 3, to reset this flag back to its original value.**
The system is now ready to be upgraded to DMA v6.4.1.6.

If the above steps are not performed prior to the upgrade to DMA v6.4.1.6 the DMA may fail to boot.

Resolved Issues

Previous Patch 5 for DMA 6.4.1 (i.e. v6.4.1.5 or v6.4.1_P5) was augmented with the following items:

Key	Summary
DMA-16960	Participants connected to slave RMX conference hear IVR waiting for chairperson
DMA-16828	CBC ciphers should be disabled Two security options have been added for the administrator. These options are located on the Security Settings page. These options will allow or prevent the system from using ciphers with the 3DES and CBC algorithms. A reboot is required after a change is made to these settings for them to be applied to the system. • For non-MSM mode, the default is to "Allow CBC ciphers" (true) and to "Allow 3DES ciphers" (true).

	• For MSM mode, the default is to "Allow CBC ciphers" (true); however, "Allow 3DES ciphers" is set to not allow (false). In MSM mode, those settings cannot be changed. IMPORTANT NOTE: 1. When CBC ciphers are not allowed, only TLS 1.2 support is available. The normal ciphers that are provided for TLS 1.0 and TLS 1.1 all contain the CBC algorithm.

Patch 6 for DMA 6.4.1 (i.e. v6.4.1.6 or v6.4.1_P6) has been augmented with the following items:

Key	Summary
DMA-16990	Rollback changes for AllowCBC and Allow3DES fields for the security settings API
DMA-16988	DMA rejecting VMR calls with temporarily unavailable.
DMA-16986 DMA-16828	DMA 6.4.1.5+ If both "Allow TLS 1.2" and "Allow CBC ciphers" are disabled at the same time, the GUI and API ports are inaccessible. CBC ciphers should be disabled Two security options have been added for the administrator. These options are located on the Security Settings page. These options will allow or prevent the system from using ciphers with the 3DES and CBC algorithms. A reboot is required after a change is made to these settings for them to be applied to the system. • For non-MSM mode, the default is to "Allow CBC ciphers" (true) and to "Allow 3DES ciphers" (true). • For MSM mode, the default is to "Allow CBC ciphers" (true); however, "Allow 3DES ciphers" is set to not allow (false). In MSM mode, those settings cannot be changed. IMPORTANT NOTES: 1. When CBC ciphers are not allowed, only TLS 1.2 support is available. The normal ciphers that are provided for TLS 1.0 and TLS 1.1 all contain the CBC algorithm. 2. The options for TLS 1.2 and CBC ciphers cannot both be unchecked (not allowed) at the same time or a warning will be presented. (Provided by DMA-16986)
DMA-16982	Issue encountered: Unable to limit maximum number of participants that can join on a scheduled pooled VMR by enabling 'Maximum participants' option Workflow & Workaround: If a scheduled conference that uses the DMA is created by a product other than the DMA, all changes to the conference room should be made on the other product before the scheduled start time. If a change to 'Maximum participants' is made after the conference start time it will not take effect because the conference is already in progress.
DMA-16980	DMA Upgrades to 6.4.1.5 can result in a permanent reboot loop
DMA-16852	DMA SNMP settings does not update FW config when changing transport protocol
DMA-16823	Restoring backup after re-image in 6.4.x DMA does not restore the SSL certificate ending up with a self-signed cert. Workaround A - Configure an IP address prior to loading backup 1. Prior to restoring backup on a freshly loaded image, assign basic IP

	information (through console/ssh) 2. Restore backup. Correct server cert will be assigned after reboot, along with the rest of the restoration. Workaround B - Restoring backup while DMA is still configuring as DHCP 1. Restore the backup through the UI. 2. DMA reboots TWICE. 3. After the second reboot, observe that all the configuration/data is restored, sans the server certificate, which has reverted to a self-signed cert. 4. Restore the backup again. DMA will only reboot ONCE this time, and all will be correctly configured, including the server certificate.

Known Issues

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

Key	Summary
DMA-16975	DMA sending a SIP response to a SIPS request
DMA-16976	DMA is reporting alerts 4011 for multiple RMXs. DMA should stop affecting the MCU score when a redialing CSS call fails
DMA-16978	Territory failover using DMA 6.1.x, numerous ~10 second Full GCs noted.
DMA-16981	DMA supercluster | Embedded DNS did not function properly when DMA went down
DMA-16983	Memory leak caused by SIP INVITEs being looped back to the source DMA running 6.1.x
DMA-16989	DMA does not forward ACK msg leading to content failures between SfB clients (o365 users) and Polycom in direct VMR dialing (VMR presence scenario)
DMA-16991	The defined DMA Skype Roster cascade link name intermittently flip from the defined name to conf_id@domain.com if CSS or Softblade is used in the RealConnect conference.
DMA-16995	CDR reports "Display=1" for an immersive call that has three endpoints in the origEndpoint column

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 6.4.1.5, 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*		*Intermediate Upgrade*	*Toggle Security Settings Required?*		*Final Upgrade*	*New License Required?*
5.0.x, 5.1.x, 5.2.0	→	5.2.1[1]	→	6.2.2.2[2]	→	6.3.2.4[3]	Yes.	→	6.4.1.6[4]	Yes.
5.2.1, 5.2.2.x, 6.0.x			→	6.2.2.2[2]	→	6.3.2.4[3]	Yes.	→	6.4.1.6[4]	Yes.
6.1.x, 6.2.x					→	6.3.2.4[3]	Yes.	→	6.4.1.6[4]	Yes.
6.3.x							Yes.	→	6.4.1.6[4]	Yes
6.4.x							Yes.	→	6.4.1.6[4]	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 6.3.2_P4_Build_231355-full.bin to upgrade to 6.3.2.4
4. Use 6.4.1_P6_Build_240027-full.bin to make the final upgrade to version 6.4.1.6.

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. **Note/Warning:**
   These steps are mandatory prior to upgrading to DMA v6.4.1.6.
   Failure to follow these steps may cause the DMA to fail to boot.

   A. If upgrading from a DMA version 6.2.x or earlier, it is mandatory to perform Intermediate Upgrades listed in the "Supported Upgrade Paths" table to get to DMA v6.3.2.4.

   B. Once the DMA is at or above v6.3.2.4, perform the following before upgrading to DMA v6.4.1.6:
      1) Go to Admin -> Local Cluster -> Security Settings
      2) Toggle the 'Ignore SIP "critical" privacy flag'
      3) Click "Update"
      4) Repeat steps 2 & 3, to reset this flag back to its original value.

   The system is now ready to be upgraded to DMA v6.4.1.6.

   If the above steps are not performed prior to the upgrade to DMA v6.4.1.6 the DMA may fail to boot.
2. 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:
RealPresence DMA System Operations Guide 6.4.0
http://support.polycom.com/content/dam/polycom-support/products/UC-Infrastructure-Support/collaboration_conferencing_platforms/user/en/DMA-6-4-0-Operations-Guide.pdf

3. Download the upgrade file for DMA v6.4.1_P6
4. Login to DMA and navigate to Maintenance > Software Upgrade
5. Select "Upload and Upgrade" and choose the upgrade file
6. DMA processes and applies patch
7. 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.

Hypervisor Environments for Virtual Edition

Products Tested with this Release

Product	*Tested Versions*
Hypervisor Environments for Virtual Edition Polycom supports mixed Hyper-V and VMware environments, but has not tested all configurations and combinations.	
VMware vSphere®	5.5, 6.5
VMware vCenter® Server	5.5, 6.5
Microsoft Hyper-V	Microsoft Windows Server 2016, Datacenter edition