Patch Release Notes

Polycom® RealPresence® Distributed Media Application™

Release label:	9.0.1_P2	(9.0.1_P2_Build_6134-full.bin)
Built on version:	Polycom DMA System v9.0.1.1	
Released files:	ISO, OVA, Hyper-V and the upgrade file	

Purpose

DMA v9.0.1.2 contains all fixes from all previous releases to date, up to and including v6.4.1.8 and v9.0.1.1. Please refer to those Release Notes for a complete list.

The Resolved Issues section below captures issues that were fixed in this release.
The Known Issues list captures issues that were reported since the last DMA GA release.
Recommended workarounds are tabulated where applicable.

Resolved Issues

Patch 2 for DMA 9.0.1 (i.e. v9.0.1.2 or v9.0.1_P2) has been augmented with the following items:

Key	Summary
EN-42410	Cache value in Postgress for callaudit is causing id sequence CDR data to be lost
EN-42435	GUI sip peer count is bad when configuring a peer with FQDN and Auto Detect transport
EN-58548	DMA 6.x to 9.0 upgrade, the DNS search domains field should place a default for the DNS search domains field on upgrade if one is not present.
EN-64966	DMA rejects a tel-uri provided in the FROM field from a SIP INVITE if parameters are included in the "<>" brackets
EN-65753	Local users with provisioner role receive error "You have insufficient permissions to perform the operation. Please logout and login again" when navigating to Monitoring > Active Calls
EN-66000	DMA hardcodes SIP scheme on tel: uri if incoming request URI is set to sip:
EN-66561	Incorrect user copy of conference room ids and aliases
EN-70368	Multipoint call is established when a transfer is executed
EN-73320	DMA 9.0.0.3 and also 9.0.1 allows you to change the log level from Debug to Verbose debug on web UI but the server.log print remain as debug, no verbose print which usually shows “TRACE”.
EN-73592	Conference subscription behaves differently depending on supercluster host
EN-75515	PCC gateway not joining RealConnect call when GS escalating P2P call to AVMCU conference by adding DMA VMR
EN-76216	CDRs show distorted data when MCU media server is not available.
EN-76744	2 nodes in a DMA 9.0.1 supercluster stopped responding to SIP signaling
EN-78338	API query /api/rest/conference-rooms?username=M* does not work

EN-78667	ELITE: DMA > Some calls in the CDR are associated to the incorrect conference.
EN-78680	9.0.1 DMA cannot create conferences on RMX if the user's name contains certain characters
EN-83617	Avoid generating a new self-signed cert if we already have a sufficient cert This is primarily to help customers who have upgraded from DMA 6.x to DMA 9.x or later. During upgrade, HA is disabled, and the user must re-enable it. During this re-enabling, currently, a new self-signed cert is generated. Instead, when enabling HA, DMA should examine any current cert it has, and only generate a new self-signed cert if the existing one is insufficient for the desired configuration. DMA will need to check that the current real and virtual IPs exist in the cert. If they do, DMA should attempt to use the existing cert. It should provide the user a warning that the cert is being re-used, and allow the user to verify the cert. If the IPs are not in the current cert, then it cannot be re-used, and the DMA shall generate a new self-signed cert as usual. If a new cert will be needed then the GUI should have a warning to the user about certificate changes.
EN-83630	Restore of Backup Should Allow Certificates Only Option When restoring a backup that includes configuration data, the GUI will provide an additional checkbox on the "Confirm Restore" dialog. The first Restore checkbox, "IP network, certificate, security and licensing configuration" works as described and has not changed. The second Restore checkbox, "Certificates only; no IP network, security or licensing configuration" will restore just certificates. The first two checkboxes cannot be selected together, however, neither is required to be selected. If the second box is selected, all of the certificate data in the selected backup file will be restored to the system. Cert data will also be restored if first box is checked along with network, security settings, etc.
EN-84564	DMA removes the min-SE field from a forwarded 422 SIP message.
EN-84721	Direct dial SIP calls are being gatewayed to H323 calls when SIPContactsInternal is empty
EN-85896	DMA No Longer Starts Up if in FIPS Config
EN-86593	DMA removes all Enterprise Passcode imported from AD after a cache refresh
EN-87526	API query /api/rest/users does not support wildcard
EN-87693	DMA removes Enterprise Passcode when updating enterprise user data
EN-90018	Virtual edition needs patching against spectre/meltdown vulnerabilities

Known Issues

Issues that have been identified since the release of DMA 6.4.1.8 and DMA 9.0.1.1 but are not included in 9.0.1.2 are aimed to be fixed in a future release.

Key	Summary
EN-68666	Instructions about restore of a 6.4 HA backup to a 9.0 HA DMA have not been updated with new workflow. WORK-AROUND: 1. Write down all the network information (IP, domain, routes, NIC information) for your secondary node of your HA pair. 2. Take a backup of your HA pair and download it. If you intend to use the same IPs on your new system, it is best to shutdown these DMAs before continuing. 3. On your 9.x DMAs, keep them in single-server configuration. On the DMA meant to be the first/primary node, apply the backup as a restore (through the USB stick or the DMA GUI). 4. On the DMA meant to be the second node, manually enter your network information from #1, and allow it to reboot. 5. Once both DMAs are up, manually configure HA mode on the primary node. Allow it to reboot. 6. After the primary node DMA reboots, go back to the HA page and choose "Configure peer". Follow the steps in the popup window and click OK. 7. Allow the second/secondary node DMA to reboot. 8. Once the secondary node is back up, you should have a DMA HA pair that contains the information from your old set.
EN-75557	DMA Displays Scrambled Exception When Trying to Configure a Supercluster Peer as an External SIP peer
EN-82093	After successfully scheduling a VMR with date, start and end time, if you edit the VMR, large arrows show on the schedule and integration page but numbers are missing. Happens on IE11 only.
EN-82138	Scheduled VMR is displayed on the UI even after the VMR has expired or been deleted
EN-83859	Inaccurate MCU Alarm status (mcuState) displays in DMA Integration > MCU page
EN-86211	Hostname gets swapped after upgrade of HA DMA cluster from 6.4.x to 9.0.1.1
EN-91771	RPRM scheduled pooled conferences with chairperson configured using a DMA template that points to an RMX profile are NOT launched by DMA as required
EN-92264	DMA fails to clean up mixer if terminated VMR was a secured conference on RMX, making the VMR unreachable afterwards

Prerequisites/Configuration Considerations

- See table below for Supported Upgrade Paths
- When upgrading from 6.4.x to a 9.0.x the system will not preserve the call history information. To keep this data, backup the databases, upgrade the DMAs, and then restore the databases.

Supported Upgrade Paths

Current Version	*Intermediate Upgrade*	*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]	→ 6.4.1.1[3]	→ 9.0.1.2[5]	Yes.
5.2.1, 5.2.2.x, 6.0.x		→ 6.2.2.2[2]	→ 6.4.1.1[3]	→ 9.0.1.2[5]	Yes.
6.1.x, 6.2.x, 6.3.x			→ 6.4.1.1[3]	→ 9.0.1.2[5]	Yes.
6.4.0.x, 6.4.1, 6.4.1.1, 6.4.1.2				→ 9.0.1.2[5]	Yes.
6.4.1.3, 6.4.1.4, 6.4.1.5, 6.4.1.6, 6.4.1.7			→ DELL-HW-Utility[4]	→ 9.0.1.2[5]	Yes.
6.4.1.8				→ 9.0.1.2[5]	Yes.
9.0.0, 9.0.0.1, 9.0.0.2			→ DELL-HW-Utility[4]	→ 9.0.1.2[5]	No.
9.0.0.3 9.0.1 9.0.1.1				→ 9.0.1.2[5]	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_P1_Build_232148-full.bin to make the final upgrade to version 6.4.1.1.
4. Use DELL-HW-Utility.bin DELL-HW-Utility for R630s.
5. Use 9.0.1_P2_Build_6134-full.bin to make the final upgrade to version 9.0.1.2

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.

Upgrading Superclustered or High Availability (HA) Systems

If you have superclustered or High Availability systems to upgrade, note the following requirements:

- If you upgrade the RealPresence DMA system from any of the supported 6.4.x and earlier versions, you must break your superclusters before you upgrade to version 9.0.1.x. After you upgrade each system, you can reestablish your supercluster connections.

- If you upgrade a RealPresence DMA system HA pair from version 6.4.x, you can upgrade one of the systems or the virtual IP and the upgrade will be applied across both HA systems. After the upgrade, you must re-enable the systems as an HA pair.

- If you upgrade a RealPresence DMA system HA pair from version 6.4.x, the certificate requirements for HA may change. Because of this change, the DMA system certificate may be reset to a default self-signed certificate when the systems are re-enabled for HA on 9.0.x. As the certificates may be reset, be prepared to issue a new DMA system certificate from your Certificate Authority after the systems have been re-enabled for HA.

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:
   RealPresence DMA System Operations Guide 9.0.0.2

   http://support.polycom.com/content/dam/polycom-support/products/UC-Infrastructure-Support/management_scheduling/user/en/dma-operations-9-0-0.pdf
2. Before continuing, ensure the intermediate upgrade using the DELL-HW-Utility Release Notes are followed if applicable.
3. Download the upgrade file for DMA v9.0.1_P2
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

The RealPresence DMA system OVA is configured to require 146 GB hard disk capacity, which Polycom has set for standard installations. To increase the required hard disk capacity, create a VM instance with the desired hard disk capacity and install the system using the RealPresence DMA system ISO file.

Note: The only benefit to having a larger hard disk capacity is the ability to store more log files.

Products Tested with 9.x Releases

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, 6.0, 6.5
VMware vCenter® Server	5.5, 6.5
Microsoft Hyper-V	Microsoft Windows Server 2016, Datacenter edition

Upgrading a RealPresence DMA Version 6.4.x System Configured for Use with a RealPresence Access Director System

Versions of the RealPresence DMA system prior to version 9.0.x supported SIP guest dialing. A RealPresence Access Director System could be configured to send "guest" (unauthorized) SIP calls to the RealPresence DMA system in such a way that the RealPresence DMA system

would invoke an alternative, unauthorized dial plan. The RealPresence Access Director system could be configured to prepend a prefix and the RealPresence DMA system would recognize that prefix and direct the call to the unauthorized dial plan. This RealPresence DMA system version 6.4.x feature was configured in Signaling Settings > SIP Settings. This SIP setting is not available in version 9.0.x, but you can achieve the same effect by using the following procedure.

RealPresence DMA System Configuration

Version 6.4.x and 9.0.x of the RealPresence DMA system have different configuration settings related to SIP guest dialing.

Version 6.4.x

- Unauthorized dial plan with dial rules U1, U2, etc.
- Authorized dial plan with rules A1, A2, etc.
- Signaling settings with the unauthorized prefix (for example, 77) and "strip prefix" optionally enabled.

Version 9.0.x

The Signaling Settings page has been split into separate H.323, SIP, and WebRTC signaling pages. The SIP Settings page does not have an option to configure unauthorized prefixes. Any unauthorized port settings in a RealPresence DMA 6.4 system will carry over during the upgrade to the 9.0.x system.

When upgrading from a version 6.4.x system, Version 9.0.x includes two predefined dial plans: Default Dial Plan, with dial rules A1, A2, etc., and Guest Dial Plan, with dial rules U1, U2, etc.

Step 1. Duplicate the Guest Dial Plan Rules Within the Default Dial Plan

After upgrading to version 9.0.x, you need to duplicate all the Guest Dial Plan rules within the Default Dial Plan.

1. Go to **Service Config > Dial Plan > Dial Plans.**
2. In the Guest Dial Plan, select the first dial rule (U1).
3. Under **Actions**, click **Edit Dial Rule**.
4. Note all the settings in the dial rule:
   a Description
   b Action
   c Other items configured within the rule
   d A preliminary script (if one exists) and if it is enabled.
5. Add a corresponding dial rule in the Default Dial Plan and configure the values of the rule:
   a Description
   b Action
   c Other items configured within the rule
   d The preliminary script (if applicable), enabled or disabled.

6 Move the rule to the **top** of the Default Dial Plan.

7 Repeat the preceding steps for each rule (U2, etc.) in the Guest Dial Plan.

8 In the Default Dial Plan, insert a new dial rule, **Block**, between the rules duplicated from the Guest Dial Plan and the rules that were already in the Default Dial Plan. The Default Dial Plan should then look like the following:

- U1
- U2
- ...
- Block
- A1
- A2
- ...

The dial rules in the Guest Dial Plan can remain there. They won't be referenced; but if calls are made to an unauthorized port, the dial plan will correctly handle them.

Step 2. Create Preliminary Scripts for the Guest Dial Plan and Block Rules

After you duplicate all the Guest Dial Plan rules within the default dial plan, configure the following changes in the RealPresence DMA version 9.0.x system.

1 Using a copy of the model script, create a preliminary script for each of the Guest Dial Plan rules and the Block rule.

2 Make the following changes to the model script for each rule:

a Replace the "77" prefix with the prefix defined in the RealPresence DMA version 6.4 system. Ensure that you set the "strip_the_prefix" option to false if the prefix should NOT be stripped.

b If a preliminary script was defined for any of the U1, U2, etc., dial rules on the RealPresence DMA 6.4.x system, insert that script into the middle of the copy of the model script you created for the duplicate of the dial rule within the Default Dial Plan.

The newly-added Block rule will not have a counterpart on the RealPresence DMA 6.4 system, but it MUST have the model script in version 9.0.x.

Results

Using preliminary scripts to direct guest traffic on the RealPresence DMA system via a prefix has the following outcomes:

- The incoming SIP calls distinguished by prefix will be directed to the Default Dial Plan, so the dial rules for these calls must be in the Default Dial Plan.
- The preliminary script detects whether there is a prefix in the dial string. If there is not, the script directs the system to skip the dial rule.
- The preliminary script can optionally strip the prefix before passing the DIAL_STRING to the dial rule.
- If the RealPresence DMA 6.4 system had a preliminary script, it is invoked only if the prefix was found, and has been (optionally) stripped.

- The Block dial rule is needed to assure that any calls with prefixed dial strings do not fall through to the Authorized dial rules (A1, A2, etc.).

Limitations:
If there are multiple prefixes with different logic regarding stripping (for example, 77 is stripped but 66 is not), that is beyond the scope of this process.

Model Script
Use the following model script to create a preliminary script for each of the guest dial rules and Block dial rule.

```
// use this dial rule preliminary script with any initial dial rules that should apply to guest calls sent to DMA from RPAD with a prefix.


// after all the initial dial rules, add an additional dial rule, with action = Block.  This will keep guest calls from hitting the non-guest dial rules.


//  REPLACE the 66|77 below with the list of guest prefixes that is configured on your RPAD and recognized in your DMA, separated by vertical bars.
//  If you have only one prefix, (e.g., 77) you can write it as (77) without a vertical bar.
// This version always strips the prefix.  If you need a version that *does not* strip the prefix, change the value of "strip_the_prefix" to false.

var GuestPrefix = '(66|77)';
var strip_the_prefix = true;

var strippedDialString = strip_prefix(DIAL_STRING, GuestPrefix);

if (strippedDialString == DIAL_STRING) {
  // no stripping occurred, so there was no prefix.  skip this dial rule.
  DIAL_STRING = strippedDialString;
  return NEXT_RULE;
}

// stripping occurred, so this dial string had a guest prefix.  remove it and process this dial rule.
if (strip_the_prefix) DIAL_STRING = strippedDialString;

// ------------------------------

// IF THERE IS ANY MORE PRELIMINARY SCRIPT LOGIC, IT SHOULD GO BETWEEN THE DASHED LINES.

// ------------------------------
```

```
return;

// this function returns the stripped dial string.  If it is unchanged, there is no prefix.

function strip_prefix(dial_string, prefix) {

  var sipRegEx = new RegExp("^(sip[s]?:)" + prefix);
  // try stripping from SIP.

  var stripped = dial_string.replace(sipRegEx,"$1");
  if (stripped != dial_string) return stripped;

  // DMA 6.x does not support Guest Dialing/Unauthorized dial plans for H.323.  The following code could be used if a customer wants to implement guest dialing by prefix for H.323.

  // try stripping from H.323.
  // whether or not any stripping occurred, return whatever the replace returns.

  // var h323RegEx = new RegExp("^((h323:)?)" + prefix);
  // return dial_string.replace(h323RegEx, "$1");

  // this return is not needed if H.323 stripping is included; but is necessary if the H.323 code is commented out.
  return stripped;
}
```

APPENDIX A: EN-75564 System Ports Table Change request: DMA 9.0.0.2 Operations Manual > Web Browsers > System Ports

System Ports

The following table lists the inbound ports that may be open on the Polycom RealPresence DMA system, depending on signaling and security settings, integrations, and system configuration.

Note that the DMA system's ephemeral port range is 20000-35999 for communication with external SIP devices. The H.323 stack uses ephemeral ports from a different range.

RealPresence DMA System Inbound Ports

Port	Protocol	Description
22	TCP	SSH. Only available if Linux console access is enabled.
53	TCP/UDP	DNS. Only available if the embedded DNS server is enabled.
80	TCP	HTTP. Redirects to 443 for access to management interface (IPv4). Redirects to 443 for access to RealPresence Platform API (IPv4 and IPv6). HTTP access is not allowed. Disabled in enhanced security mode.
123	UDP	NTP. Only available if an NTP server is specified in Time Settings.
161	UDP	SNMP. Default port; can be changed or disabled.
443	TCP	HTTPS. Access to management interface (IPv4).
1719	UDP	H.323 RAS. Default port; can be changed.
1720	TCP	H.323 H.225 signaling. Default port; can be changed.
5060	TCP/UDP	Unencrypted SIP. Default port; can be changed or disabled; additional unencrypted ports can be added.
5061	TCP	SIP TLS. Default port; can be changed; additional encrypted ports can be added.
5986	TCP/TLS	Used for WinRM 2.0 communication during Polycom contact creation in Active Directory.
8080	TCP	HTTP. Redirects to 443 for access to management interface (IPv4). Redirects to 443 for access to RealPresence Platform API (IPv4 and IPv6). Used for uploading upgrade packages and backups. During upgrades, the progress page is served from this port. Disabled in enhanced security mode.
8443	TCP	HTTPS. Access to management interface (IPv6) and RealPresence Platform API (IPv4 and IPv6). Redirects to 443 for access to management interface (IPv4).
8989	TCP	Supercluster communication.
36000-61000	TCP	Used by the H.323 stack. Some of these ports are used as ephemeral ports when the RealPresence DMA system initiates a connection and others are used as inbound ports.