Patch Release Notes

Polycom® RealPresence® Distributed Media Application™

Release label:	9.0.1_P1	(9.0.1_P1_Build_4771-full.bin)
Built on versions:	Polycom DMA System v9.0.1	
Released files:	ISO, OVA, Hyper-V and the upgrade file	

Purpose

DMA v9.0.1.1 contains all fixes from all previous releases to date, up to and including v6.4.1.8 and v9.0.1. 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 1 for DMA 9.0.1 (i.e. v9.0.1.1 or v9.0.1_P1) has been augmented with the following items:

Key	Summary
EN-27046	Calls rejected when conference is ending
EN-28012	RPD/RPM doesn't follow RPRM Site-link bandwidth when call with Debut
EN-41777	Sometimes recording status of WebRTC client is wrong and the ECS gateway keep connecting to the VMR even all the participants have ended calls.
EN-59159	If a SIP call gets Cancelled quickly CANCEL fails and the call never gets cleaned up
EN-59160	License checking for forked calls does not occur until one of the callees answers.
EN-59161	CDRs from a Realconnect conference have the conference ID in the confDisplayNameList field.
EN-59164	CDR Extension Fields not populating for SIP dial out calls
EN-59574	Changing network settings of a node in a HA cluster using the USB configuration may result in that node being put into an invalid state. This can result in that node falling out of the cluster and HA and networking settings being put in an invalid state, requiring that HA cluster be set back up manually.
EN-59800	Room ID and Alias generation will generate a room ID that's already taken.
EN-60411	Admin should be warned of FIPS/TLS 1.2 conflict
EN-61063	RealConnect conferences with external Skype systems are not displaying the Cascade Roster Indicator
EN-62744	Add more MCU alerts
EN-63351	DMA shouldn't send RPWS-ECS-Gateway as a participant to RPRM during DMA pooled/ad hoc conference.

EN-63762	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.
EN-63780	A significant percentage of SIP/UDP Registrations are not being processed, resulting in retransmissions
EN-63870	Need the ability to send an offerless invite to EP (upstream) after the VEQ instead of sending the offerless invite to the RMX
EN-64243	H.323 calls into VMR created by OTD automatically ask for Chairperson password
EN-64489	H.323 dial-outs from RMX Manager fail to be recorded in Conf History, APIListener, 4575 notifications if RMX is 2/3 full
EN-64593	DMA 9.0 sets the expires parameter incorrectly in SIP register responses
EN-64678	Long running H.323 calls (many months) can cause the DMA to run out of memory
EN-65083	"RealPresence Resource Manager" page of DMA cannot get information about time
EN-65961	H.323 calls from CUCM to DMA failing
EN-66357	All backup and restore functions were blocked after reboot on DHCP system. The server's host file was corrupted by the DHCP update script by adding the host alias in front of the host FQDN. DMA rejects the host entry if the first element after the IP address is not the FQDN
EN-67275	DMA setting of the DH public key size should remain unchanged during an upgrade. NOTE: Upgrading to DMA 9.0.1.1 from a previous DMA 9.0.x release, the value will now default = 1024. However, in this release, there is now an option in the GUI for the customer to reconfigure this field if desired.
EN-67276	User should be able to set the DH public key size in the GUI NOTE: disabling DHE ciphers or changing DH public key size to 2048 will prevent logjam vulnerability.
EN-67473	Allow multi-select, to terminate calls, for Pinned Calls and Active Calls.
EN-68625	On the active node of an HA pair, the NIC IPv4 address is stored as the virtual instead of as the physical
EN-68645	Unable to assign roles to AD imported group
EN-68738	A configuration that included routes fails to fully take effect on a restore.
EN-70374	The EKU 1.3.6.1.5.5.8.2.2 is not mapped in 9.0 which causes all certificate action to fail after a cert with this EKU is uploaded
EN-72796	DMA never rolls or purges /var/log/secure
EN-73106	DMA declines recurring conferences with no end time from Outlook Plugin.
EN-73174	Endpoints & cascade link was disconnected upon initial call setup connection
EN-73886	Exchange Server integration page territory field defaults to a blank line
EN-74034	Conference room id that includes characters causes an exception
EN-74039	After delete a site in the RPRM site topology, the site is still shown in the DMA site topology
EN-74652	Users with expired passwords can't change their password

EN-76031	DMA 9.0.1 responds to preflight OPTIONS requests incorrectly
EN-76415	GUI - Add User - Get a stack trace instead of a password incompliance error message
EN-77711	DMA refuses any H.323 LWRRQ when H.323 device authentication is enabled
EN-77963	Attempt to delete a territory results in a ProximoAdminException

Known Issues

Issues that have been identified since the release of DMA 6.4.1.8 and DMA 9.0.1 but are not included in 9.0.1.1 are aimed to be fixed in a future release.

Key	Summary
EN-61063 EN-63762	This is not a Polycom bug. RealConnect conferences with external Skype systems are not displaying the DMA defined Cascade Roster Indicator. The displayed name in an External Skype system RealConnect call is = the value set in the External Skype server.
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	DMA - 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-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-70368	The Trio 8800 establishes a multipoint conference with the GroupSeries systems when it attempts to transfer a call.
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-75557	DMA Displays Scrambled Exception When Trying to Configure a Supercluster Peer as an External SIP peer
EN-75564	Web access is not redirected to port 8443, need documentation change. Refer to **Appendix A** of this Release Notes Document.
EN-76216	CDRs show distorted data when MCU is not available.
EN-76744	2 nodes in a DMA supercluster stopped responding to SIP signaling
EN-78338	API query /api/rest/conference-rooms?username=M* does not work at DMA version 9.0.1
EN-78667	Some calls in the CDR are associated to the incorrect conference.
EN-78680	DMA cannot create conferences on RMX if the user's name contains certain characters
EN-79864	Rollback of HA'ed 9.0.1 to 6.4.0 left the DMA without a valid SSL certificate Workaround: Reset the network using the USB gui or Reset the SSL key manually by logging into the shell.

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]	→ 9.0.1.1[5]	Yes.
5.2.1, 5.2.2.x, 6.0.x		→ 6.2.2.2[2]	→ 6.4.1.1[3]	→ 9.0.1.1[5]	Yes.
6.1.x, 6.2.x, 6.3.x			→ 6.4.1.1[3]	→ 9.0.1.1[5]	Yes.
6.4.0.x, 6.4.1, 6.4.1.1, 6.4.1.2				→ 9.0.1.1[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]	→ 9.0.1.1[5]	Yes.

Current Version	*Intermediate Upgrade*	*Intermediate Upgrade*	*Intermediate Upgrade*	*Final Upgrade*	*New License Required?*
6.4.1.8			→	9.0.1.1[5]	Yes.
9.0.0, 9.0.0.1, 9.0.0.2		→ DELL-HW-Utility[4]	→	9.0.1.1[5]	No.
9.0.0.3 9.0.1			→	9.0.1.1[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_P1_Build_4771-full.bin to make the final upgrade to version 9.0.1.1

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_P1
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 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.