Avaya Communicator for Android Release 2.1.1

Release Notes

Issue 1.0
17th *March* 2015

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's gents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Website:
http://www.avaya.com/support

License
USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT. Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)
Named User License (NU). Customer may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Product.
Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud
"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention
If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:
http://www.avaya.com/support

Trademarks
Avaya, the Avaya logo, and COMPAS are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site:
http://www.avaya.com/support

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:
http://www.avaya.com/support

Table of Contents

Overview

This release letter is intended to inform all end users of Avaya Communicator for Android features, caveats and known issues available in 2.1.1 release.

Avaya Communicator for Android - Release 2.1.1 – What's New

Avaya Communicator for Android 2.1.1 provides the following new features:

- **Server Identity Validation** - Avaya Communicator for Android includes implementation of server identity validation on all secure connections. If the user uses the application to connect to the VoIP, PPM, Client Enablement Services, XMPP, LDAP, Avaya Multimedia Messaging, Auto-configuration, Web Collaboration, or SSO servers, Avaya Communicator for Android performs hostname verification to ensure communication with the correct server.
- **Cellular voice for all calls option –** Removed the configuration option "VoIP over Cellular Data". This feature is currently a binary on/off switch that prevents registration when the cellular data network is used. Introduce a new configuration option called "Use VoIP for calls" with the following menu options:

    - Always
    - Only over WiFi
    - Never

- **Make Avaya Communicator call from other apps** - A method for 3rd party applications residing on the same device, to initiate a call (click to call) with Avaya Communicator Android
- **Private Trust Store -** The private trust store includes the CA certificates that can be used to validate certificates of the various servers.

Inherited from previous release (Avaya Communicator for Android 2.1)

- VoIP Mid call handling features
- Consultative Transfer and conference
- Feature toggles for: Send All Calls, EC500, Call forward all calls, Call forward busy/do not answer.
- Call Handoff – Move calls VoIP to cellular and vice versa
- Multiple Device Access (MDA) Compatibility
- VoIP call recovery – Avaya Communicator for Android will attempt to maintain your active call across network changes
- SM failover
- ActiveSync search – corporate directory search without CES
- Aura 6.2 FP4 Support
- Auto Configuration - Administrative lock to prevent local modification to settings
- SIP Telephony with Aura 6.2
- One-X CES support (Visual voicemail, Corporate directory, Call-back, Presence)
- EC500 FNE Auto-dialer
- Auto-Configuration of user settings

- SBC/VPN Support
- Presence services (enabled by One-X CES)
- Enhanced logging and crash reporting
- EC500 Station Security Code
- EC500 Call Suppression (previously called EC500 Delayed Send)
- Web Collaboration Launch
- Preservation of active call over VPN
- Support for CES "Device Specific Login"
- Support for CES "Flexible LDAP" Feature
- CES Settings: SMS Enable/Disable
- Support 46xxsettings.txt file format in service discovery
- Messaging Waiting Indicator (SIP)
- Add phones selected for simultaneous ring to menu
- Support for Android 4.x Devices

Getting Started

Review these release notes prior to starting installation of Avaya Communicator for Android R2.1.1 software

Qualified device list and Software Versions

Avaya Communicator for Android 2.1.1 FP has been tested on the following devices:

SIP only Devices:

- ✓ Samsung Galaxy S3
- ✓ Samsung Galaxy S4
- ✓ Samsung Galaxy S5
- ✓ HTC one-S
- ✓ LG Optimus G E975
- ✓ LG G2
- ✓ Sony Xperia Z2

Additional Devices for CES only configuration:

- ✓ Motorola Razr
- ✓ Samsung Note2
- ✓ LG Nexus 4
- ✓ Samsung Galaxy S3 Mini

Additional Device for EC500 only configuration:

- ✓ AOS 4.x

Note: AOS 4.0.3 or higher required for SIP operation.

Security Considerations -

Certificate Requirements-

As we evolve our portfolio of unified communications clients, Avaya is enhancing the security of our products including how digital certificates are managed. Avaya Communicator for Android introduces mandatory certificate validation for all TLS connections.

Avaya Communicator for Android uses built-in Android security features to create a trust relationship with your unified communications infrastructure. Before you deploy Avaya Communicator for Android, you will need to determine whether the servers in your unified communications infrastructure use certificates signed by a certificate authority that is trusted in the Android operating system. If your servers are using trusted certificates, no further action is required.

In order to establish TLS data connections, Avaya Communicator for Android requires a security certificate for each server that it will be connecting to. In R2.1.1, the list of servers that should be considered (depending on your specific deployment configuration) is:

- Session Manager (SM)
- Session Border Controller (SBC)
- Client Enablement Services (CES)
- Avaya Multimedia Messaging (AMM)
- HTTP server used to host the settings file for service discovery

For more detail on specific provisioning and deployment considerations, please consult the product documentation

- Administering Avaya Communicator for Android, iPad, iPhone, and Windows
- Avaya Communicator Overview and Specification for Android, iPad, iPhone, and Windows
- Using Avaya Communicator for Android

Multi-Service Deployment Considerations: -

Configuration	EC500 only	CES only	VoIP only	EC500 + CES	EC500 + VoIP	CES + VoIP	EC500 + VoIP + CES
Configuration Details	CM Off PBX Mapping = EC500	CM Off PBX Mapping = ONE-X	Standard SIP endpoint configuration	CM Off PBX Mapping = ONE-X	CM Off PBX Mapping = EC500, Standard SIP endpoint configuration	CM Off PBX Mapping = ONE-X, Standard SIP endpoint configuration	CM Off PBX Mapping = ONE-X, Standard SIP endpoint configuration
Call Origination	FNE - Idle Appearance Select	CES Call Back	VoIP	Call Origination Menu Selection (EC500 or CES)	Call Origination Menu Selection (EC500 or VoIP)	Call Origination Menu Selection (CES or VoIP)	Call Origination Menu Selection (EC500, CES, or VoIP)
FNE Support	Supported	Supported (e.g. Join Call)	Not supported	Supported	Supported	Supported (e.g. Join Call)	Supported
Simring (incoming calls)	Defined by EC500 mobile number configured on CM and whether EC500 on CM is on/off	Users use "Ring my Phones" to turn on/off calls to the mobile phone	When registered with SM SIP calls will be received	Users use "Ring my Phones" to turn on/off calls to the mobile phone	EC500 Call Suppression Logic on CM determines where incoming calls are delivered	Users use CES "Ring My Phones" to turn on/off calls to the mobile phone. EC500 Call Suppression is currently not supported in this configuration	Users use CES "Ring My Phones" to turn on/off calls to the mobile phone. EC500 Call Suppression is currently not supported in this configuration

Interoperability -

Following is the list of systems supported by Avaya Communicator for Android 2.1.1:

Product	Version
96xx Series IP Desk Phones	96x0 H.323 3.2 96x0 SIP 2.6.13 96x1 H.323 6.4,6.5 96x1 SIP 6.4
Avaya Aura® Application Enablement Services	6.3, 6.3.1 (AA 6.2 FP3), 6.3.3 (AA 6.2 FP4)
Avaya Aura® Communication Manager	6.3.2 (AA 6.2 FP3), 6.3.6 (AA 6.2 FP4), 6.3.8
Avaya Aura® Communication Manager Messaging	6.3
Avaya Aura® Conferencing	7.2.2, 8.0
Avaya Aura® Messaging	6.2, 6.3.1,6.3.2
Avaya Aura® Presence Services	6.2, 6.2.2(AA 6.2 FP3), 6.2.4(AA 6.2 FP4)
Avaya Aura® Session Manager	6.3.4 (AA 6.2 FP3), 6.3.8 (AA 6.2 FP4), 6.3.9
Avaya Session Border Controller for Enterprise	6.2.100, 6.3
Avaya Aura® Solution for Midsize Enterprise	6.2, 6.3.10
Avaya Aura® System Manager	6.3.4 (AA 6.2 FP3), 6.3.8 (AA 6.2 FP4), 6.3.10
Avaya Communicator for Windows	2.0, 2.1
Avaya Communicator for iPad	2.0
Avaya client application	6.3.1
Avaya One-X® Client Enablement Services	6.2
Avaya Communicator for iPhone	2.1
Avaya one-X® Communicator	6.2, 6.2.3
Scopia Solutions	8.3, 8.3.1
Avaya one-X® Communicator for Mac OS	2.0.4
Avaya one-X® Mobile	6.2
Avaya one-X® Mobile SIP for iOS	6.2.5
Meeting Exchange	6.2
Avaya Multimedia Messaging	2.1
Avaya Modular Messaging	5.2

Known Issues:

Sr. No.	Key	Summary	Workaround
1	FA-6528	AC Android shows "Can't Acquire Speaker or Mic to establish VOIP Call" while trying to make an outgoing call after Failback to SM from BSM.	Logout/login VoIP
2	FA-5406	Remote line doesn't show up after dropping call from AC Android (SBC) when the user bridge in from desk phone	Logout/login VoIP
3	FA-6516	Call drops after SM Failover if both endpoints are connected to Primary SM	None
4	FA-5039	Audio drops if hold/un-hold after 20+ minutes on AAC conference call with secure media (SRTP)	Disconnect and re-establish a new call
5	FA-5965	Active VoIP call may be lost when user moves form Wi-Fi to 3G and back to Wi-Fi n/w	None
6	FA-6112	Two calls active with blended audio after quickly switching between them 2-3 times	None
7	FA-6113	Scratchy noise on call made to a PSTN extension when the call is routed via a SIP trunk over SBC with the near end having SRTP and the Far end on RTP	Hold and un-hold call
8	FA-6002	After failover to BSM, warning message for limited VoIP services does not persist	None
9	FA-6261	Android O/S does not check validity period of trust anchor certificates	None
10	FA-6726	App crashes when user received/answered another incoming VoIP call when first call is extending to cellular	None

Interoperability issues:

Sr. No.	Key	Summary	Workaround / Notes
1	defsw141238	AC Android MDA bridge in scenario causes CM reset	Provided details on “Special Instructions for Admin” section Use CM 6.3 SP8 and above for MDA feature
2	FA-2826	CES mode – Callback call get disconnected instantly after answer at destination mobile when call is placed from local contact card with AAC details	Depends on CES fix ONEXCESSERVER-9473

3	FA-3381	Corporate Directory search does not return results if search term is last name and contains space character	Depends on CES fix ONEXCESSERVER-9613
4	FA-2907	AC Android voicemail total duration shown lesser than actual length of the voicemail	Depends on CES fix ONEXCESSERVER-9503
5	FA-6000	Active P2P call with AC iPad or AC Windows disconnects automatically, after AC Android client as an MDA endpoint tries to bridging-in to the call	Depends on CM MR defsw141519 CM has a patch that was tested, and the plan is to include the fix in their upcoming CM6.3.10
6	FA-5508	CES call back call using "Call Using Office/desk phone" causes call rings only on AC Android and no other phones in MDA group.	Depends on CM MR CM-3241
7	FA-4962	Flexible LDAP Fields (city and company) are not Displayed in Favorite Details	Depends on CES fix ONEXCESSERVER-9894
8	FA-4215	Mobile Phone number is not always updated in My Phone when edited in CES Phone settings	Depends on CES fix ONEXCESSERVER-9939
9	FA-5539	In MDA case (AC Android and One-X Communicator) 'Unavailable' status set on AC Android client causes messages delivered on OneXC	Depend on CES fix ONEXCESSERVER-9994 Allow One-X Communicator presence to be master by leaving mobile set to Automatic" Or set DnD directly on One-X Communicator
10	FA-6097	No voice path is observed during P2P call in Alpha SBC setup	Depend on SBC fix AURORA-5093
11	FA-5738	Hold button doesn't work on One-x communicator when the call is made from AC Android	Depend on SBC fix AURORA-4948
12	CM-3241	CES call back using deskphone is not working and call appearance display as locked on deskphone	None

Caveats

These are issues that are closed and represent notable behaviors that the GMI team should review.

Sr. No.	Key	Summary	Workaround / Notes
1	FA-5262	AMM-PS Federation: Device status not published when Android user logs in	AC Android user needs to manually change the presence status. This is limitation of CES.
2	FA-5257	Automatic Presence Status shown as offline when AC Android user logs in	AC Android user needs to manually change the

			presence status. This is limitation of CES.
3	defsw131628	EC500 call suppression feature does not work when application is ONE-X. For an incoming call user will receive two calls, one for SIP and one for CES.	Use CM 6.3 SP6 and above
4	FA-3832 defsw132344	User is unable to hold/un-hold the incoming P2P video call (initiated from one-X communicator) when 1XM call is routed using SIP trunk.	Use CM 6.3 SP5 and above
5	FA-5306, FA-5189	Samsung Note II - AC Android crashes observed during initiating P2P call, call transfer	Android OS 4.4.2 instability on Samsung Galaxy note-2
6	FA-5130	Local contacts are display after 3 to 4 minutes on Samsung Note-2, when we have 2500+ contacts.	Android OS 4.4.2 instability on Samsung Galaxy note-2
7	FA-2934	After disconnect VPN connection, status of VoIP mode is not updated as "not logged in" by displaying cross icon on dial button (It takes up to 4 minutes for app to detect VPN dropped)	There is a window of time before the status indicator will be updated to reflect the real status of the connection.
8	FA-5163	3G-VPN: Call appearance of VoIP call remains active (observed for 10 minutes) if far end user drops active call.	None
9	FA-5389	When there is active cellular call on android device and AC Android user bridge into the VoIP call on other MDA endpoint causes cellular and VoIP voice mixing.	Do not bridge into active VoIP call on another MDA device when there is cellular call on device
10	FA-5150	No voice path AC Android when there is an active call on Skype	Ensure that there are no active VoIP calls on another VoIP supported applications like Skype, Jabber
11	FA-5143	Picture taken and sent from an AC-iPad client over a P2P AMM chat session is shown as inverted on the AC-Android client.	None
12	FA-5121	Continuous ringing is on Bluetooth for cellular call when there is active VoIP call on AC Android.	None
13	FA-5017	If you enable Client Enablement Services and EC500, then pressing the EC500 button has no effect on endpoints that the application manages using the Ring Phones feature of Client Enablement Services	None

14	FA3706	Acoustic shock failure for Australia on HTC One S on handset mode	Avaya recommends that only headphones or headsets that offer Acoustic Shock Protection be used with the Avaya Communicator for Android application in conjunction with the Android device. (Such as the Jabra Supreme or the Plantronics Voyager Pro).

Special Instructions for admin –

Outlook contacts via Active Sync -

To manage/import outlook contacts via Active Sync please use following steps in release notes -

1) As per the steps provided in following link configure exchange email on android mobile device
   http://help.outlook.com/en-us/140/Dd940179.aspx
2) On AC Android go to "Settings -> Account and Services -> CES account information" and Disable CES on login page
3) Go to AC android contacts tab and select "corporate directory" in drop down list and search the required enterprise contact.

AC Android MDA bridge in scenario causes CM reset/MCD (FA-5526 P1/S1) –

Bridge in from desk phone or from AC Android causes MCD on CM when AC android client is involved in MDA scenario.

Workaround /Mitigation – Remote line appearance "Join" button disabled by default on AC Android 2.1

- The default state show the active line appearance on the tab and the call menu screen, however the "Join" button will be greyed out (disabled)
- "Join" button can only be enabled by the configuration file. This gives administrative control over the situation. They can activate the feature via configuration file if they know CM is patched/updated with fix for defsw141238.

It contains the disabling of Join unless the following is incorporated in an auto-config file…

```
{
  "accounts": [
    {
      "signaling": {
        "enable-mda-join": "1"
      }
    }
  ]
}
```

1 = Join is enabled
0 (default) = Join is disabled… the button will never enable or be usable.

46xxsettings file has the following syntax to enable MDA Join button:
Auto-config profile to enable the MDA Join button: **SET ENABLE_MDA_JOIN 1**
And the syntax to disable MDA Join button: **SET ENABLE_MDA_JOIN 0**

Installing Avaya Communicator for Android from Google Play

Procedure

- On the device, go to *https://play.google.com/store* or open the Play Store application.
- Do one of the following:
    - If you are using *https://play.google.com/store*, type Avaya Communicator in the text field and then tap the Search icon.
    - If you are using the Play Store application, tap the Search icon and then type Avaya Communicator in the text field.
- Tap the entry for Avaya Communicator.
- Tap INSTALL.

Appendix A: SIP Endpoint Provisioning

Avaya Communicator for Android is a SIP endpoint with the following configuration recommendations. Administrators shall ensure:

On SMGR:

- SMGR CM endpoint profile template is provided (for example, DEFAULT_9640SIP_CM_6_2)
- IP Softphone is enabled
- CM-ES is in the originating and terminating application sequence
- “extnd-call” feature button must added on CM extension for EC500 Call Suppression (previously called EC500 Delayed Send) feature to work
- “EC500” feature button should added on CM extension to use EC500 related features

On CM:

- On Communication Manager signaling group associated with Avaya Session Manager, set “Initial IP-IP Direct Media” to “Y”
- Set the value of “Trunk group to SM” in field "Proxy Set Rte Pat"; available in Locations on CM
- “DTMF over IP” field on “change signaling-group” should be “rtp-payload”
- Page 2 of the IP-OPTIONS SYSTEM PARAMETERS screen, set the “Override ip-codec-set for SIP direct-media connections” field to “N”.
  Note –
  1) If you have AAC 7.2 FP1 in Aura setup then please set “Override ip-codec-set for SIP direct-media connections” as Y. It’s mandatory to have this set as Y for AAC functionalities to work. But this will affect the codec preference set on CM, as SIP to SIP direct-media calls will use an audio codec based on the preference of the SIP endpoint.
  2) If you have AAC 7.2 FP2 or later in Aura setup then please set “Override ip-codec-set for SIP direct-media connections” as N.

Note –

- Minimum supported CM version 6.3 *(R016x.03.0.124.0)* as per the interoperability matrix
- EC500 call suppression and Multiple Device Access (MDA) are available only when the server installation is Avaya Aura 6.2 FP2 or later
- EC500 station security is available only when the server installation is Avaya Aura 6.2 FP3 or later
- EC500 call suppression for one-X calls is available only with CM version 6.3 SP6 and later
- Avaya Multimedia Messaging 2.1.1 support Aura FP4 and later
- SBCE 6.3 does not support CES traffic
- Use SBCE 6.3 release to avoid the PPM connection issue.

Appendix B: Acronyms

– Avaya one-X® Client Enablement Services = 1xCES

– Avaya one-X® Mobile = 1xM

– Avaya one-X® Communicator = one-X Communicator

– Avaya Aura® Communication Manager = CM

- Avaya Communicator for iPad = AC iPad

– Avaya Aura® Session Manager = SM

– Avaya Aura® System Manager = SMGR

– Avaya Session Border Controller for Enterprise = Avaya SBCE

– Avaya Aura® Conferencing = AAC

– Avaya Communicator for Android = AC Android