

Avaya Callback Assist
Release Notes

Release 4.6.2.0
December 2017

Issue 2

© 2015-2017 Avaya Inc.
All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. 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 You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "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. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY

OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Note to Service Provider

The product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

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 Toll 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 website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.
Avaya is a registered trademark of Avaya Inc.
All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Table of Content

About this document 5

New features in Callback Assist 4.6.2.0 6

Support Avaya Oceana™ Release 3.3 for SIP Agent First Strategy 6

Support Oceana Ingress VDN per Callback Configuration 6

Support HTTPS / TLSv1.2 by default via CBA Installer 6

Upgraded Tomcat Instances to Version 7.0.82 6

Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2 support 6

Installer prompts to accept Avaya's End User License Agreement (EULA) 7

Passwords are encrypted 7

Features, Enhancements and Defect Fixes included in Callback Assist 4.6.2.0 8

Known issues in Callback Assist 4.6.2.0 10

Upgrade an existing installation 12

Hardware and software requirements 12

Technical support 13

About this document

This document contains information about features and fixes delivered in Avaya Callback Assist (CBA) 4.6.2.0. This document also lists any known issues and information about getting technical support if you experience issues with Callback Assist.

New features in Callback Assist 4.6.2.0

Callback Assist 4.6.2.0 introduces the following new features.

Support Avaya Oceana™ Release 3.3 for SIP Agent First Strategy

In this release CBA supports Avaya Oceana™ deployment in SIP Agent First strategy. CBA will place an outbound call to an Oceana Ingress VDN via CBA CCXML application, and once the agent answers the outbound call, CBA will initiate another call to customer and finally agent & customer calls are merged.

Please refer to the **Avaya Callback Assist Overview and Planning** guide, **Installation and Configuration** guide and **Administration** guide for more information on the Avaya Oceana™ integration feature.

Support Oceana Ingress VDN per Callback Configuration

This is the extension to support Oceana feature in SIP Agent First and CFPQ strategies. The administrator can configure Oceana Ingress VDN per callback configuration which will override the Global Settings configuration. Please refer to the **Administration** guide for further details.

Support HTTPS / TLSv1.2 by default via CBA Installer

Now CBA Installer supports HTTPS by default. CBA Installer offers the option to have CBA configured with HTTPS with TLSv1.2 only or not (plain HTTP as today). This new option automates most of the manual post-installation HTTPS configuration steps required in release 4.6.1 or earlier releases.

Please refer to the **Installation and Configuration** guide and **Avaya Callback Assist Application Notes for SSL or TLS Configuration** for more details about the security configuration applied with this new option.

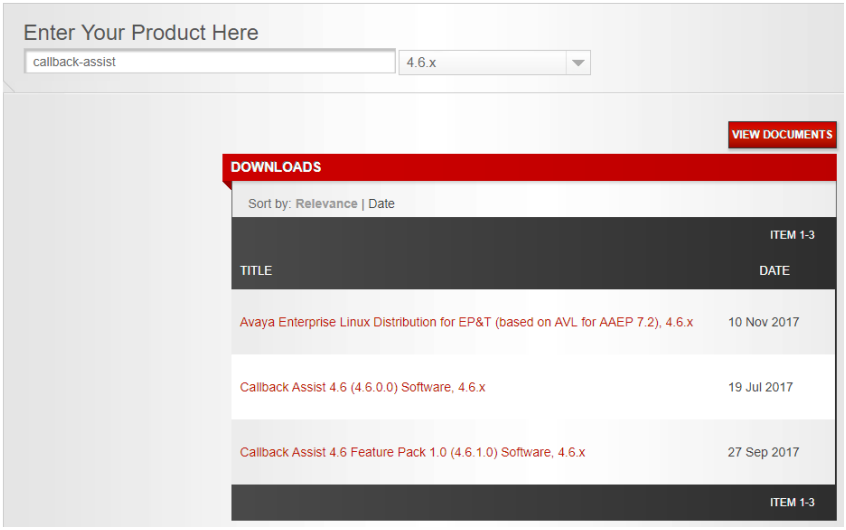
Upgraded Tomcat Instances to Version 7.0.82

Tomcat 7 instances are upgraded from 7.0.79 to 7.0.82 (Sep 29 2017), to fix CVE-2017-12617 security vulnerability. Version 7.0.82 is the latest Tomcat 7 release at the time CBA release 4.6.2 goes GA.

Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2 support

Callback Assist release 4.6.1 or higher supports Avaya Enterprise Linux for Avaya Aura® Experience Portal 7.2 (aka “Avaya Linux” or “AVL”). Callback Assist requires a slightly customized Avaya Enterprise Linux for Avaya Aura®

Experience Portal 7.2 that only changes the disk partition table. This customized distribution of Avaya Linux for CBA can be downloaded from the Avaya Support Site as Avaya Enterprise Linux Distribution for EP&T (based on AVL for AAEP 7.2):



Installer prompts to accept Avaya's End User License Agreement (EULA)

CBA installer now asks the user to accept the Avaya's EULA, at the beginning of the installation, to proceed with the installation or the upgrade. The EULA file will be available in the CBA binary extracted folder.

```
[root@server205 4.6.2]# ./callback-install.sh

************************************************************
Avaya Callback Assist Installer
************************************************************

Do you accept the Avaya's End User License Agreement ("EULA") specified in '/opt/releases/4.6.2/AvayaGlobalSoftwareLicenseTerms_final.pdf' ?
Enter 'yes' to proceed with the installation/upgrade, 'no' to terminate:
```

Please refer **Installing and configuring Avaya Callback Assist** user guide for more details.

Passwords are encrypted

Service passwords stored in configuration files (ex.: .properties files) in plain text are encrypted. Ex.: PostgreSQL 'callback' database user password. See section *Changing an encrypted Postgres password* in the **Administering Avaya Callback Assist** end-user guide for details on how to change an encrypted password and where.

Features, Enhancements and Defect Fixes included in Callback Assist 4.6.2.0

This release includes the following fixes.

Issue ID	Type	Severity	Description
CBA-6583	Bug	3-Medium	Oceana configurations tab is seen in an AACC deployment
CBA-6563	Bug	3-Medium	For every created callback request in Agent First the callback status is wrongly updated to FAILED(5) instead of in IN_IVR(2), when Real Time Messaging feature is disabled.
CBA-6561	Bug	2-High	Upgrade Failed from 4.6.1.0 to 4.6.2.0 due to Postgres FATAL error
CBA-6556	Bug	2-High	Google Authentication in the CBA Admin UI not working. Once upgraded to 4.6.1 all users asked to change the password
CBA-6527	Bug	3-Medium	EPM_OUTBOUND_WS_INVOCATION_FAILS Kafka event is not raised when EPM credentials are miss-configured in CBA
CBA-6488	Bug	2-High	Error occurs when customer is returned to queue when option 'Use Customer Entered Number as Caller ID' is checked.
CBA-6477	Bug	1-Critical	When Dynamic Routing Delivery is enabled the Offer Application is not querying the Dynamic Routing WS when an immediate callback is created.
CBA-6443	Bug	3-Medium	Minor issues in *Avaya Callback Assist Application Notes for SSL or TLS Configuration* user guide
CBA-6337	Bug	3-Medium	EWT value as -1 (65534) shown in the pending reports when no Oceana (CC Elite) agents are staffed
CBA-6255	Bug	2-High	Tomcat ddapps and tomcat webcallback didnt come up automatically after server reboot
CBA-6206	Bug	2-High	Security - User credentials are sent in clear text
CBA-6186	Bug	3-Medium	Callback status not updated to INITIATION_FAILED by engine on BusinessException in

			RequestTaskTemplate
CBA-5312	Bug	3-Medium	Remove references to Confluence URLs from the FAQ/Troubleshooting user guide
CBA-6546	Enhancement	3-Medium	Clarify input parameters of create immediate/scheduled WS APIs for all signatures in the WS API guide.
CBA-6523	Enhancement	3-Medium	CBA is not sending callbackGuid manadatory tag in Dynamic Routing WS request
CBA-6460	Enhancement	3-Medium	Add an entry to the FAQ & Troubleshooting guide showing how CBA uses AAEP ports
CBA-6448	Enhancement	3-Medium	Enhance CBAExternalVXMLLauncherSample integration documentation
CBA-6412	Enhancement	3-Medium	Upgrade Tomcat 7 instances from 7.0.79 to 7.0.82 or higher release, to fix CVE-2017-12617 vulnerability
CBA-6400	Enhancement	3-Medium	All service passwords cannot be stored in plain text in configuration files but encrypted
CBA-6391	Enhancement	3-Medium	Update Avaya Callback Assist Application Notes for SSL or TLS Configuration with Pending Callbacks Summary Report changes
CBA-6369	Enhancement	3-Medium	When enabling "Callback Offer Application as an Orchestration Designer Module" setting a Warning prompt should be presented
CBA-6356	Enhancement	3-Medium	The user should accept Avaya's End User License Agreement ("EULA") in order to install or upgrade CBA
CBA-6352	Enhancement	3-Medium	Oceana Service Metrics should be queried using the priority specified in the informed context
CBA-5930	Enhancement	3-Medium	Customize the AAEP 7.2 Avaya RedHat Linux (AVL) distribution (create new ISO file)
CBA-6456	Story	3-Medium	As a Supervisor I need to be able to assign an Oceana Ingress VDN per callback configuration
CBA-6322	Story	3-Medium	HTTPS/TLSv1.2 supported by default in a fresh install
CBA-6321	Story	3-Medium	Support Agent First on Oceana 3.3.x

Known issues in Callback Assist 4.6.2.0

The following issues were not fixed in this release:

Issue ID	Severity	Description
CBA-6567	3-Medium	When using the Offer Application as a module the INCOMING_CALL, INCOMING_CALL_REDIRECTED_TO_QUEUE and CUSTOMER_DROPPED Kafka events are not raised.
CBA-6564	3-Medium	CALLBACK_REQUEST_CREATED Event is not raised when creating a callback from web
CBA-6525	3-Medium	Time zone values in date time fields taken from AAEP in Kafka events must be converted to be in the CBA global setting time zone
CBA-6491	4-Low	For various columns in CallBack Configuration Management in Admin UI, the sorting feature is not working properly.
CBA-6486	3-Medium	CBA Engine service cannot be started manually if not done in proper order
CBA-6362	3-Medium	Add callback configuration name to real-time Kafka events
CBA-6336	3-Medium	Stopping CBA BSR Server service failed on CBA 4.6.1.0 (SIP Legacy HA)
CBA-6117	4-Low	CTI - Callback Engine Server IP on global setting must not accept invalid format of IP address
CBA-5322	3 – Medium	Warn CBA Alarm is not raised when No AAEP Ports are available when calling the Customer in CF PQ
CBA-5321	3 – Medium	Audit log - Reorder questions - no reference to callback configuration
CBA-5320	3 - Medium	Audit log - No reference to callback name/id when adding web questions to an existing callback
CBA-5319	3 - Medium	Audit - Each new generation of the audit log file will reorder logged lines if they have the same timestamp
CBA-5315	3 – Medium	Audit log - No information regarding callback configuration when updating a wav file
CBA-5314	3 – Medium	Audit - Calling Rules Management updates are difficult to understand

CBA-5312	3 – Medium	Remove references to Confluence URLs from the FAQ/Troubleshooting user guide
CBA-5308	4 – Low	Error message for improper WS timeout does not make sense
CBA-5294	3 – Medium	Remove 10 symbols limiation from Dialstring text input field in dialing rules
CBA-5290	3 – Medium	If User Is Disabled/Deleted While Being Logged In, On User's Next Page Load the Administration Page Remains Unresponsive
CBA-5210	3 – Medium	No entry shown in Audit log when changing a callback type from voice to composite
CBA-4495	4 – Low	Description of "Merge the Agent Call on to the Customer Call" advanced tab setting has incorrect reference in user guide,
CBA-4457	3 – Medium	Intermittent error "Application error has occurred, you session has reset" on CBA login screen
CBA-857	4 – Low	Incorrect timezone displayed on CBA BSR Configuration page
CBA-693	4 – Low	Copyright text is not matching on prelogin and postlogin page of CBA admin
CBA-692	4 – Low	Add role page missing text "Report" for Pending Callbacks Cancellation
CBA-579	3 – Medium	SIP CF: “Please hold while I call the customer” message is played to the agent twice
CBA-578	3 – Medium	CBA Admin: User account is not locked once maximum login attempts is reached
CBA-577	3 – Medium	Adding a new Polling VDN/Queuing VDN pair requires Polling Service restart
CBA-389	3 – Medium	Installer should ignore http_proxy variable

Upgrade an existing installation

Please check *Installing and configuring Avaya Callback Assist* guide for detailed information about upgrading Callback Assist.

- Callback Assist 4.1.8 and above requires higher hardware specifications than 4.1.7.1 and below. Check the **Linux Shared Memory, Hardware requirements** and **Network Latency** sections of *Installing and configuring Avaya Callback Assist* guide before upgrade.
- Callback Assist 4.4.0.0 and above require the security certificate of all the EPMs installed in CBA. Refer the "*Add AAEP Security Certificate to CBA*" section of "Installing and configuring Avaya Callback Assist" document.
- Callback Assist 4.4.1.0 and above 64 bits OS doesn't require to install 32-bit compatibility libraries. If it is already installed it can be removed by using the following command:
  - ***sudo yum remove glibc.i686***

  This command will uninstall 32-bit libraries. This step is not mandatory.
- Whoever using Internal CBA WebLM and upgrading Callback Assist from 4.4.1.0 and below to Callback Assist 4.5.0.0 and above, they have to recreate the licenses used by the WebLM server. The existing licenses that is installed in internal CBA WebLM 4.7.1 (CBA 4.4.1.0 and below) will not work if we upgrade WebLM 6.3.17 (CBA to 4.5.0.0 and above), since the host id generation logic is different from these two versions.

  Even though Mac ID of the WebLM server is same, the Host ID generated by the WebLM server is different and it is tightly linked with WebLM server. Existing licenses installed in WebLM 4.7.1 should be recreated with the new Host ID (given by WebLM 6.3.17) after the CBA upgrade. Contact APS team to get the new license and that can be used for CBA.

Hardware and software requirements

For information on setting up the required environment configuration, see the following sections in the *Installing and Configuring Avaya Callback Assist guide*.

- Browser Requirements
- Hardware Requirements
- Software Requirements
- Network Latency

Technical support

Support for CBA is available through Avaya Technical Support.
If you encounter trouble with CBA, perform the following tasks:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, contact Avaya Technical Support by one of the following ways:

- Logging on to the Avaya Technical Support Web site.
- Calling or faxing Avaya Technical Support at one of the telephone numbers in the Support Directory listings on the Avaya Support Web site.

You may be asked to email one or more files to Avaya Technical Support for analysis of your application and its environment.

Note:
If you have difficulty reaching Avaya Technical Support through the above URL or email address, please visit the Avaya Web site for further information.

When you request technical support, provide the following information:

- Configuration settings
- Usage scenario, including all steps required to reproduce the issue.
- Screenshots, if the issue occurs in the Administration Application, end-user web site or Portal clients.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

Tip:

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Support Web site.

For information about patches and product updates, see the Avaya Support Web site.