Avaya Session Border Controller for 10.1.2.1 Release Notes

Release 10.1.2.1
Issue 1
December 2023

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 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 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 Web site: http://support.avaya.com

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)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

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://support.avaya.com

Trademarks

Avaya and the Avaya logo 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://support.avaya.com

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://support.avaya.com

Table of contents:

Overview

This document provides information about the enhancements, upgrade support, platforms supported, software download information, list of fixed, known issues and workarounds in ASBC Release 10.1.2.1.

Note: 10.1.2.1 release is only applicable for non-JITC customers. JITC customer must not install this software.

Admin and Deployment guide for 10.1.2

Title	Support Site Link
Avaya Session Border Controller Overview and Specification	https://support.avaya.com/css/P8/documents/101079520
Deploying Avaya Session Border Controller on a Hardware Platform	https://download.avaya.com/css/public/documents/101079507
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	https://support.avaya.com/css/P8/documents/101079504
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	https://support.avaya.com/css/P8/documents/101079490
Deploying Avaya Session Border Controller on a Microsoft Azure Platform	https://support.avaya.com/css/P8/documents/101079500
Deploying Avaya Session Border Controller on a Google Cloud Platform	https://download.avaya.com/css/public/documents/101079484
Upgrading Avaya Session Border Controller	https://support.avaya.com/css/P8/documents/101079514
Administering Avaya Session Border Controller	https://support.avaya.com/css/P8/documents/101079522
Maintaining and Troubleshooting Avaya Session Border Controller	https://support.avaya.com/css/P8/documents/101079518
Working with Avaya Session Border Controller and Microsoft Teams	https://support.avaya.com/css/P8/documents/101079528
Working with Avaya Session Border Controller Multi-Tenancy	https://support.avaya.com/css/P8/documents/101079526
Working with Avaya Session Border Controller Geographic-Redundant Deployments	https://support.avaya.com/css/P8/documents/101079524
Avaya Session Border Controller Release Notes	https://download.avaya.com/css/public/documents/101087747
Avaya Session Border Controller Port Matrix	https://support.avaya.com/css/secure/documents/101086143

Software Downloads

Software downloads are available at following links:
https://support.avaya.com/downloads/
https://plds.avaya.com

File Name	PLDS ID	MD5SUM	Remarks
sbce-10.1.2.1-84-23872-5e3226b2ad36c61e8d442d6d59d97580.tar.gz	SBCE0000338	5e3226b2ad36c61e8d442d6d59d97580	Upgrade package for upgrade 10.1.2.1 release ***Note:*** 10.1.2.1 release is only applicable for non-JITC customers. JITC customer must not install this software.
sbce-10.1.2.1-84-23872-5e3226b2ad36c61e8d442d6d59d97580.tar.gz.asc	SBCE0000339	1e84eb89b8b4c3958faa170f2751429e	Signature file to be used to upgrade to 10.1.2.1 release
sbce-10.1.2.1-84-23872-signatures.tar.gz	SBCE0000340	f13b6c5f8cb1c2edd2611b7190809b85	Key Bundle to validate. RPM signatures
sbce-10.1.2.1-84-23872_uberutility-2a0c639a2f47119e7187c423411afc24.tar.gz	SBCE0000342	2a0c639a2f47119e7187c423411afc24	Uberutility tool to clean disk space

Pre-Requisite Before Upgrade

Mandatory Hotfix before Upgrading from 10.1.2.0 to 10.1.2.1

Platform/Hardware Type	GUI Based upgrade	CLI based upgrade
VMs	Supported after installing the Hotfix	Direct upgrade with/without Hotfix
Dell 3240	Supported after installing the Hotfix	Direct upgrade with/without Hotfix
Dell R340	Supported after installing the Hotfix	Direct upgrade with/without Hotfix
Dell R640(ACP3 & ACP5)	Supported after installing the Hotfix	Direct upgrade with/without Hotfix
VEP 1425	Not Supported	Direct upgrade (Must not install Hotfix)

GUI based upgrade from SBC 10.1.2.0 to SCB 10.1.2.1 **mandates** installing of Hotfix (Hotfix details given below) on SBC 10.1.2.0 software (EMS and SBCs) before initiating upgrade. For CLI upgrade this Hotfix is optional. Hotfix must not be installed Software running on VEP 1425. VEP 1425 only support CLI based upgrade.

Here are the Hotfix details (PLDS ID : SBCE0000335)(Please refer the PSN # PSN006213u) ::
Patch hotfix1: sbce-10.1.2.0-64-23285-hotfix-08282023.tgz
md5sum: 67d2278460f89cdbcfb420ee1457d9d5

Steps to Install Hotfix and key bundle (not applicable for VEP1425):
Stop the application using command “/etc/init.d/ipcs-init stop“and please wait for all the process to be stopped.

1. Copy the tar file “sbce-10.1.2.0-64-23285-hotfix-08282023.tgz” to /home/ipcs directory.

2. Untar the patch tar file

```
#tar -zxvf sbce-10.1.2.0-64-23285-hotfix-08282023.tgz
```

3. Go to directory sbce-10.1.2.0-64-23285-hotfix-08282023

```
#cd sbce-10.1.2.0-64-23285-hotfix-08282023
```

4. To apply the patch, run below command

```
# sh install_hotfix.sh
```

5. After applying the patch, system must be rebooted.

6. After Step#5, Install “sbce-10.1.2.0-64-23285-signatures.tar.gz” file key bundle on EMS GUI (download signature file from support site)

Disk space check before Upgrade

Check the disk space using “**df -h”** command as shown below. If **Use %** is more than 50% then cleanup the disk space using Uberutility tool available in PLDS. Please make sure /archive and /boot partition usage are less than 40% for successful upgrade.

Example:

```
[root@ACP5-SBC2 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs         94G     0   94G   0% /dev
tmpfs            94G   28K   94G   1% /dev/shm
tmpfs            94G  3.1G   91G   4% /run
tmpfs            94G     0   94G   0% /sys/fs/cgroup
/dev/sda6       9.4G  6.5G  2.9G  70% /
/dev/sda12      330G  165G  165G  51% /archive
/dev/sda8       4.7G   33M  4.7G   1% /tmp
/dev/sda11      106G  4.3G  101G   5% /usr/local
/dev/sda5       9.4G  679M  8.7G   8% /var
/dev/sda2       4.7G  3.4G  1.4G  72% /home
/dev/sda1       951M  654M  298M  69% /boot
/dev/sda9       4.7G  417M  4.3G   9% /var/log
/dev/sda7       4.7G  1.1G  3.7G  22% /var/log/audit
tmpfs            19G     0   19G   0% /run/user/0
tmpfs            19G     0   19G   0% /run/user/1001
```

Note: Do not run the pre-upgrade-check script of uberutility tool for upgrading to SP. pre-upgrade-check script is only applicable for upgrading to Feature Pack (FP) and major release. Recommendation of running pre-upgrade-check script in SBC 10.1.2 document is primarily for upgrading to FP or major release. For upgrading to SP, this note overrides SBC 10.1.2 Document for running the pre-upgrade-check script.

Steps to run Uberutility tool for disk space cleanup

1. Download the Uberutility package from support site and copy to /home/ipcs on EMS and SBC’s and run following Linux commands
2. mkdir /usr/local/ipcs/temp (If already present this directory then clear this: rm -rf /usr/local/ipcs/temp/*)
3. tar -xzvf sbce-10.1.2.1-84-23872_uberutility-2a0c639a2f47119e7187c423411afc24.tar.gz -C /usr/local/ipcs/temp/
4. cd /usr/local/ipcs/temp
5. ./sbc-diskspace-cleanup.py

Supported Upgrade Path

Only ASBC 10.1.2(UEFI) is allowed for direct upgrade to 10.1.2.1. All other SBC version/releases should be upgraded to 10.1.2 before upgrading to 10.1.2.1

Note: Follow the mandatory instructions before upgrading to 10.1.2.1

Supported Platforms for Upgrade

The following platforms are supported for upgrading to ASBC 10.1.2.1 release:

1. Dell 3240
2. Dell R340
3. VMWARE ESXI Version 6.7/7.0
4. Dell R640 (ACP 3 and ACP 5)
5. VEP1425
6. Azure, AWS, Nutanix and GCP

List of Known Issues with Workarounds

Issue Summary	Workaround
Intermittent issue, where Jade media service stopped running on the secondary SBC after enabling (if disabled previously) the transcoding/transrating feature flag on EMS-SBC.	Restart the application on secondary SBC.
Ipcs-version command output on SBC (standalone), shows duplicate line for PCF module	Ignore, No impact to the service
Intermittent issue, where SNMP traps are not sent outside of EMS.	Restarting spiritAgent Run the Command: systemctl restart spiritAgent
Intermittent issue, where "SIP Statistics" viewer is showing "SNMP communication error	Run the below command on SBC. "/usr/local/ipcs/icu3/workaround/ResetSnmpConfig.sh"

List of fixed issues

Key	Summary
AURORA-32361	SNMP is not working on 10.1.2 GA/HF
AURORA-32315	ipcsServerHeartbeat need to have more meta data related to server IP and Name
AURORA-31589	Audio lost both way after 15 mins if the call following Re-INVITE from Service Provider
AURORA-32137	iPhone NG911 call with AMR-WB call in and has only one-way audio.
AURORA-31598	call being dropped by Teams due to missing ICE candidates in hold/unhold in refer with replaces.
AURORA-31046	Fail to import CA certs in bundles (20-30) in one file.
AURORA-31626	SSYNDI restart when using sipp to sending an abnormally long Record-Route option with 255 additional routes.
AURORA-32035	SBCE is getting crash on BYE if sending by Callee and URI Group is configured in Routing profile.
AURORA-31489	Packet capture is not working on fresh install 10.1.2.
AURORA-32056	PPM Mapping-SBC removed transport Name and transport Port in getHomeCapabilitiesResponse.
AURORA-32053	syntax error in bulkelogtrimmer script result disk full on 10.1.2+Hf1
AURORA-31698	Sigma Script not working post upgrading to 10.1.2
AURORA-31279	ICE candidates are not sending back in 200 OK during call-forwarding scenarios
AURORA-31264	offload transcoding suddenly stop after running for a period of time

AURORA-31717	SBC crashed with PRACK msg from SP, probably due to Validation failure
AURORA-31023	Jade_MS stopped working
AURORA-31577	SBC is violating SIP RFCs while modifying Contact header URI.
AURORA-31788	Syslog shows as failed state when you add any new syslog configuration
AURORA-28608	SNMP user created in primary EMS is not showing up in teh secondary EMS /var/net-snmp/snmpd.conf
AURORA-30190	SBCE takes 3.5 hours to load all interface IP results outage
AURORA-31613	In 10.1.2, more easily to get disk full
AURORA-31542	SSYNDI memory Leak, almost exhaust in a day , server need to reboot daily for restoring service
AURORA-31282	Failed to install scrubber pkg in 10.1.2
AURORA-31165	Missing CSP/ Security header in https message in revers proxy
AURORA-31263	Max call legs 100000 reached error is coming and service restored after SBC reboot
AURORA-31258	ASBCE is crashing while processing the 200 ok message
AURORA-31210	Ssyndi.log keep on increasing in size, log rotation seem no effect on it
AURORA-31094	unable to perform log collection from GUI
AURORA-31147	SNMP sub agent stops responding, fd count increase to threshold value
AURORA-29583	Once upgrade to 8.1.3.1, AAfD in telecommuter mode has one way audio
AURORA-31217	SBCE is crashing while processing the BYE(forked call).
AURORA-31037	SBCE is crashing while processing 200 OK of Subscriber msg
AURORA-31947	Firewall Whitelist/Blacklist API does not work on separate SBCE
AURORA-29029	security threat for exposing application name(nginx) not implementing the security header.

Note: 10.1.2.1 also support External Transcoding with AMS.

List of Open issues

Key	Summary
AURORA-32426	SBCE: Not handling "BYE" correctly if Invite with Replaces is there and SP is disconnecting Call.
AURORA-32425	SBCE: Active Calls Count in SIP Statistics is different than Server Flow's Active Call
AURORA-32374	Dynamic Licensing use one license for registered J-phone compare to one-x communicator even with no call.
AURORA-31938	EASG script doesn't allow user input and didn't handle warning msg properly and work on secondary EMS
AURORA-32118	Missing HTTP Strict-Transport-Security Header in nginx.conf

Security Upgrades

CVEs	Advisory	Synopsis	Publish Date
https://access.redhat.com/security/cve/CVE-2023-4911 https://access.redhat.com/security/cve/CVE-2023-4813 https://access.redhat.com/security/cve/CVE-2023-4806 https://access.redhat.com/security/cve/CVE-2023-4527	https://access.redhat.com/errata/RHSA-2023:5455	Important: glibc security update	2023-10-05
https://access.redhat.com/security/cve/CVE-2023-38408	https://access.redhat.com/errata/RHSA-2023:4419	Important: openssh security update	2023-08-01

https://access.redhat.com/security/cve/CVE-2023-34969	https://access.redhat.com/errata/RHSA-2023:4498	Moderate: dbus security update	2023-08-07
https://access.redhat.com/security/cve/CVE-2023-32067	https://access.redhat.com/errata/RHSA-2023:3584	Important: c-ares security update	2023-06-14
https://access.redhat.com/security/cve/CVE-2023-29469 https://access.redhat.com/security/cve/CVE-2023-28484	https://access.redhat.com/errata/RHSA-2023:4529	Moderate: libxml2 security update	2023-08-08
https://access.redhat.com/security/cve/CVE-2023-24329	https://access.redhat.com/errata/RHSA-2023:3781	Important: python38:3.8 and python38-devel:3.8 security update	2023-06-22
https://access.redhat.com/security/cve/CVE-2023-23908		Important: microcode_ctl security update	2023-08-22
https://access.redhat.com/security/cve/CVE-2023-2283 https://access.redhat.com/security/cve/CVE-2023-1667	https://access.redhat.com/errata/RHSA-2023:3839	Moderate: libssh security update	2023-06-27
https://access.redhat.com/security/cve/CVE-2023-20593	https://access.redhat.com/errata/RHSA-2023:5245	Moderate: linux-firmware security update	2023-09-19
https://access.redhat.com/security/cve/CVE-2023-0286 https://access.redhat.com/security/cve/CVE-2023-0215 https://access.redhat.com/security/cve/CVE-2022-4450 https://access.redhat.com/security/cve/CVE-2022-4304	https://access.redhat.com/errata/RHSA-2023:1405	Important: openssl security update	2023-03-22
https://access.redhat.com/security/cve/CVE-2022-36227	https://access.redhat.com/errata/RHSA-2023:3018	Low: libarchive security update	2023-05-16
https://access.redhat.com/security/cve/CVE-2022-34903	https://access.redhat.com/errata/RHSA-2022:6463	Moderate: gnupg2 security update	2022-09-13
https://access.redhat.com/security/cve/CVE-2022-2929 https://access.redhat.com/security/cve/CVE-2022-2928	https://access.redhat.com/errata/RHSA-2023:3000	Moderate: dhcp security and bug fix update	2023-05-16
https://access.redhat.com/security/cve/CVE-2022-24407	https://access.redhat.com/errata/RHSA-2022:0658	Important: cyrus-sasl security update	2022-02-23
https://access.redhat.com/security/cve/CVE-2022-1927 https://access.redhat.com/security/cve/CVE-2022-1897 https://access.redhat.com/security/cve/CVE-2022-1785	https://access.redhat.com/errata/RHSA-2022:5813	Moderate: vim security update	2022-08-02
https://access.redhat.com/security/cve/CVE-2022-1586	https://access.redhat.com/errata/RHSA-2022:5809	Moderate: pcre2 security update	2022-08-02
https://access.redhat.com/security/cve/CVE-2022-1271	https://access.redhat.com/errata/RHSA-2022:4991	Important: xz security update	2022-06-13
https://access.redhat.com/security/cve/CVE-2023-3776	https://access.redhat.com/errata/RHSA-2023:5244	Important: kernel security, bug fix, and enhancement update	2023-09-19
https://access.redhat.com/security/cve/CVE-2023-27536	https://access.redhat.com/errata/RHSA-2023:4523	Moderate: curl security update	2023-08-08
https://access.redhat.com/security/cve/CVE-2023-29491	https://access.redhat.com/errata/RHSA-2023:5249	Moderate: ncurses security update	2023-09-19
https://access.redhat.com/security/cve/CVE-2022-39377	https://access.redhat.com/errata/RHSA-2023:2800	Moderate: sysstat security and bug fix	2023-05-16

		update	