Avaya Session Border Controller for Enterprise Release 6.2.1

Release Notes

Release 6.2 FP1
Issue 5
December 2013

Table of Contents

Upgrade process to 6.2.1.Q07

From 6.2.0 releases prior to 6.2.1 release

Single step Upgrade to 6.2.1.Q07 can be done from 6.2.0 Q48 or Q58. An SBC upgrade can be done using the GUI (System Management -> Updates->Upgrade from uploaded file).

If the customer has any load prior than 6.2.0 Q48. Upgrade is a two stage process.

1. Upgrade the system to 6.2.0 Q48 or Q58
2. Upgrade the system to 6.2.1.Q07.

Rollback to Release 6.2.0 involves following manual steps:

1. Follow the normal rollback procedure using the GUI.
2. After the upgrade finishes, open an SSH connection to the EMS.
3. Run rollback-tomcat.sh (attached).

rollback-tomcat.sh

From 4.0.5 releases to 6.2.1 release

Upgrade to 6.2.1.Q07 is a two stage process.

1. Upgrade from 4.0.5 to 6.2.0 Q48 or Q58.
2. Upgrade to 6.2.1.Q07 using the GUI (System management -> Updates->Upgrade from uploaded file).

Roll back to 4.0.5 release is not supported.

New features and enhancements

Following new features are added.

Multi-Device Access (MDA)

Avaya Aura® introduced the feature Multiple Device Access (MDA) in Avaya Aura 6.2 Feature Pack 2. In this feature, a user with same number can access the call using devices of different capabilities. All devices of the user will ring for incoming call. A user can answer with best device or mobile paired device. After the call answered, all remaining devices stop ringing. If the user wants to use a device with better capability, the user can join in to the existing call using that device. This action creates a conference on ACM, and it is expected for the user to drop manually from its older device whose capability it is no longer using. This procedure is known as handoff. However, this mechanism has issues in video calls or in conferences using Avaya Aura® Conferencing as Avaya Aura® Conferencing provides other rich conferencing features which is affected by this mechanism. In case of an Avaya Aura® Conferencing hosted conference, the MDA device which joined the call last is active and all other devices which joined in call earlier are dropped.

No configuration is required on SBC.

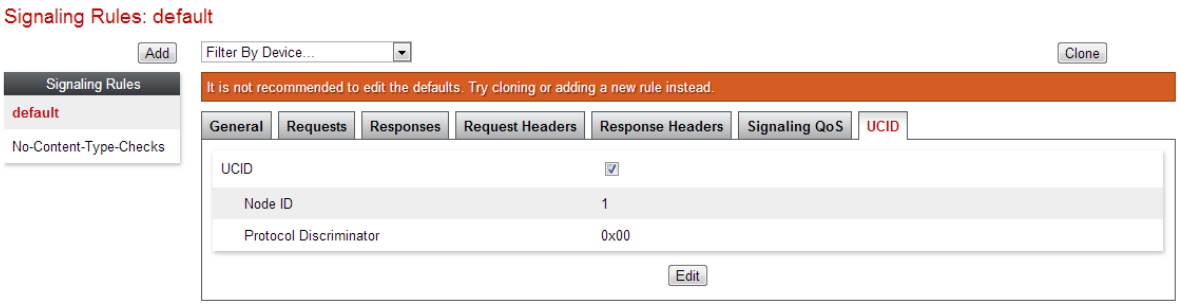
UCID

Avaya SBC-E 6.2 FP1 can add a Universal Call Identifier (UCID) in the signaling of an inbound trunk call. UCID is Avaya proprietary call identifier used for correlation of a call in a Contact Center application like in any Work Flow Optimization (WFO) and Call Recording. The usage is applicable at non-SIP interfaces of CTI using various means of JTAPI, DMCC and other proprietary Avaya mechanisms to provide an abstraction of call topology to a Contact Center application and UCID is applied to monitor and control such a call from a Contact Center application. UCID is also used to track call history in a Contact Center application.

UCID configuration is part of the Signaling rules:

Node Id: Node Id is an administrable value that uniquely identifies a network node within a customer's network. A node Id is two bytes (signed) long and can be a value between one and 32767. Zero is not a valid network node.

Protocol Discriminator: The default value is set to user specific 0x00. Usually it should not be changed.



IP Office remote worker solution

Enhancements are made to support remote worker solution for IP Office.

The following IP Office soft-clients (SIP end points) are supported with ASBC-E 6.2 Feature Pack 1:

- Flare Experience for iPad
- Flare Experience for Windows
- one-X Mobile Preferred VoIP client for Android
- one-X Mobile Preferred VoIP client for iOS

Capacity enhancement – RSS

SIP trunking capacity on the Dell R210II and Dell R210II XL is scaled from 2000 to 5000 maximum simultaneous non-encrypted sessions. If encryption is used, 1000 simultaneous sessions are allowed. For remote worker there is no change as the unencrypted sessions allowed are 2000 or the encrypted sessions allowed are 1000.

No configuration is required on SBC.

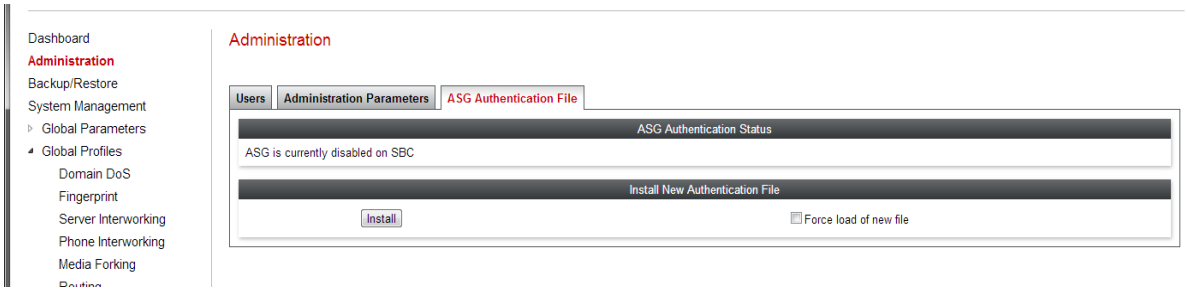
Access Security Gateway (ASG) based login for GUI and CLI

Access Security Gateway (ASG) based user login for GUI and CLI is supported in this release by all Avaya SBC-E family of products.

Protecting passwords to prevent unauthorized use of maintenance and administration logins is a key element in securing an Enterprise Communication System (ECS). On Avaya ECS products, all passwords used by Avaya services personnel are used only once – for a single access attempt. After each access attempt (success or failure), a new password must be used. This security prevents anyone from obtaining a password and reusing it later. A one-time-password is actually a response to a random challenge to a person seeking to gain access on a given login.

This random challenge/response mechanism for one time access to the Avaya resources is provided by Avaya Security Gateway (ASG) using AES encrypted secret key. Without knowledge of the secret ASG encryption key, an intruder cannot, on the first try, rapidly provide the proper response to the challenge generated by the ASG feature.

ASG Configuration is administered from GUI Administration->ASG Authentication File. See *Administering Avaya Session Border Controller for Enterprise* for detail steps.



Video SRTP

Support for Video SRTP added in this release. When SRTP is configured for video make sure to disable "Encrypted RTCP" usually "Encrypted RTCP" is enabled by default.

GRIPS

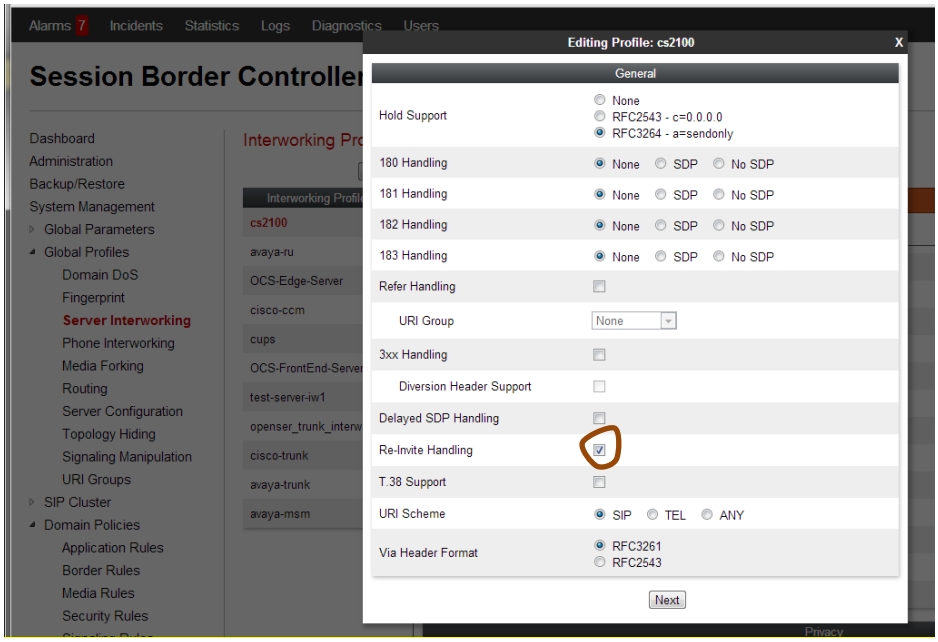
10778 SBC-E - action required to stop reINVITEs during refresh

Some trunk service providers do not allow such reINVITEs traverse their network for the following reasons:

- Avoids any message flooding.
- Any re-invite implies a change in the media.
- This behavior is considered to be bounded within the IP PBX so that the network should not be impacted by it.

The aim is to reject the re-INVITE related to the same C-seq or another parameter that allows us to discard the messages on the SBC. The re-invite is allowed only for fax services, thus when the Re-invite contains the T.38 attribute it is routed across the network. In other words, any change in the media (or SDP) SBC allows the re-INITVE to trunk provider. If and their network is not able to support this make sure media rules are configured with appropriate codecs.

This feature can be enabled by enabling the “Re-Invite Handling” in the server interworking profile.



11128 SIP REFER translation to SIP Invite

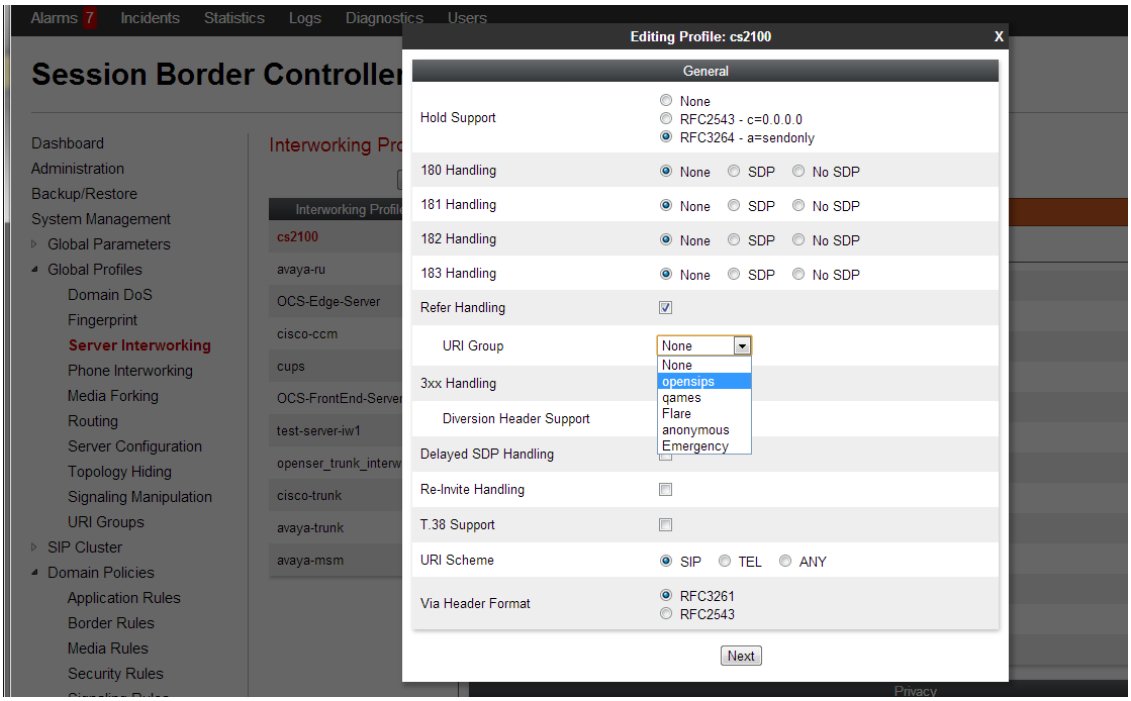
REFER needs to be converted into INVITE and go towards CPE and other REFER needs to go towards the network based upon Refer-To URI group. Refer-To Criteria URI group is configured in server interworking profile.

Also, enable Change Call-ID option in the Trunk server interworking profile -> Advanced options

For an Avaya Remote Worker solution, the Change Call-Id option should not be enabled. In this release, the same SBC device cannot be used for both Remote worker and Trunk if REFER handling is enabled for trunk server. This limitation will be fixed in an upcoming service pack.

Please note AST-2 based transfer is not supported by many trunk providers. If AST-2 is enabled in Communication Manager, use the following workaround configuration:

- SIGMA SCRIPT is mandatory (Sigma script needs to be modified per customer to suit the deployment details).
- Topology hiding for REFER-by/Refer-TO should not be enabled



Security enhancements

New security defaults for DOS/DDOS

In this release, all the DOS/DDOS related defaults are updated based on the Avaya SBC-E security configuration and best practices guide.

Scrubber

Scrubber package is enhanced to eliminate some false positives. As part of upgrade latest package are copied to EMS to "`/usr/local/ipcs/icu/scrubber_files`" directory, and not automatically applied part of the upgrade. Copy these files to local PC using scp or sftp and follow the procedure in the *Administering Avaya Session Border Controller for Enterprise* guide to install these new packages.

Features not supported in this release

AST-2 transfer for trunk

In this release AST-2 transfer is supported only for remote workers. For trunks, it is not supported because of the known Communication Manager issue (defsw130462 and defsw130568). In the case of the trunk deployment, configure Communication Manager to use only AST-1.

Security features

Following security features not supported in this release:

- Finger printing
- Media anomaly detection

List of the issues fixed in 6.2.1.Q07 from 6.2.1.Q05

Key	Summary
AURORA-1149	Transfer fails when Refer Handling is enabled towards callserver
AURORA-1320	The SBC-E (Micro) could not handle the flooding attack using different message types using Lava tool
AURORA-1370	SBC - Route - URI - Unsuccessful call from Sipgate.co.uk
AURORA-1411	Customer BET365 SNMP get requests fail intermittently - oampserver restart required to wake up the service again
AURORA-1495	After SIP Trunk has an outage, SBC sends runaway REGISTER
AURORA-1528	Trigger: SBC is masking when Session Manager failover occurs preventing remote SIP endpoints from detecting when Limited Service conditions exist.
AURORA-1631	Trigger - Making an administrative change to RELAY for Prognosis RTCP monitoring requires full reboot,
AURORA-1635	No call preservation after SM fail over
AURORA-1654	SBC-E removing XML portion of Multipart SIP headers
AURORA-1666	IPO scrubber: Need separate scrubber package for IPO remote worker, for basic meetme call Rulenames 84, 17, 85, 86, 21 & 82 are triggered with Aura scrubber package.
AURORA-1669	No Audio between remote and internal phones when Shuffling is Enabled in CM
AURORA-1680	Conversion from SIP INFO to RFC 2833 leaves out Media Description
AURORA-1688	REFER handling not working 6.2.0Q48
AURORA-1708	Flare Experience 1.2 : No Audio when Video enforced with only SRTP in SBC
AURORA-1718	SBC is changing transport from sips to sip if SDP audio coming with port 0
AURORA-1719	End-End TLS/SRTP: There is no media between SBC Remote User Flare clients [R1.1], when media shuffling is enabled on CM - Y/N combination.
AURORA-1729	Device swap is only available if configured devices(SBC) are only in commissioned status and in same build as EMS
AURORA-1731	Hear ring back tone forever when calling into CM Messaging from SBC
AURORA-1733	Media lost on long duration calls when converting SRTP to RTP
AURORA-1746	By default Media Anomaly Detection(MAD) is enabled in GUI Media Rules
AURORA-1748	After SBC HA failover one-x mobile remote clients are not getting registered to new primary
AURORA-1751	Fax T38 calls not working after upgrade from 4.05 to 6.2.0
AURORA-1766	Cannot upload ASG file on HA system
AURORA-1777	Clear button not working in Incident Viewer
AURORA-1782	Trigger - Attempted to upgrade SBC-E from Q62 to Q64 & 3 of the SBCs failed

List of the issues fixed in 6.2.1.Q05 from 6.2.0 SP5

Key	Summary
AURORA-640	Request to change the way SBC handles SUBSCRIBE messages during conference call establishment
AURORA-918	OUT OF DATE JAVA VERSION
AURORA-920	Clone not available in Endpoint Policy Groups to create independent profile based on existing defaults
AURORA-1002	Call walk Dos incident is detected but has a display error in the GUI
AURORA-1012	Out of Date Apache2 version on UCSec
AURORA-1394	Subscriber flows configured with "Methods Allowed Before REGISTER" with more than one value are missing after upgrade to Q48
AURORA-1433	TLS Management -" Peer Verification Required" blocks 96X1 phones
AURORA-1465	GUI allows install of CA cert even when the CA has an expired date
AURORA-1474	Clicking from high numbered Application Policy to Media Interface fails to load profile data
AURORA-1497	No voice path B to A when A un-pause the video in SBC call
AURORA-1504	Call transfer involve UPDATE fail.
AURORA-1510	One way audio path for calls in TLS/SRTP - Lync SIP trunking Testing
AURORA-1513	Modification on sip uri group and uri manipulation is not taking effect until cold restart
AURORA-1514	Uri manipulation is not working for TEL uri
AURORA-1518	CP - Flare 1.2.0.0[Job-1.103] - Unable to de-escalate video call to audio call from Internal Flare client, during Ext-Int and Int-Ext video call scenarios.
AURORA-1531	UCID feature on SBC
AURORA-1533	User is not able to transfer a call between TLS A - SBC TLS X and SBC TLS X - TCP B
AURORA-1546	vi: Call drops when PSTN client calls through SBC SIP Trunk to AAM Auto Attendant transfer to CMES client
AURORA-1547	SBC in Ottawa GSC Lab (135.20.249.74) incorrectly adds 'avaya-sc-enabled' tag to contact URI in NOTIFYs
AURORA-1552	SSYNDI process did not come up after 4 times SBC Application Restart from GUI
AURORA-1561	HBO CS1K remote worker issue: 1140 SIP set registers then sends TCP keep alive. The SBC doesn't forward the TCP keep alive to the CS1000.
AURORA-1562	SM ignore the INIVTE (in call transfer after REFER), because rport param in the invite first VIA header towards transfer target.
AURORA-1564	6.2 FP1: Feature request: Add RSS support to Dell-based SBC
AURORA-1565	6.2 FP1 - GRIP 11128 - REFER translation & GRIP 10778 RE-INVITE handling
AURORA-1569	JavaScript Documentation Cleanup and Static Analysis
AURORA-1571	6.2 FP1 - Server DoS and Domain DoS Changes
AURORA-1576	SBC support for MDA Feature
AURORA-1584	ASG Authentication 6.2FP1
AURORA-1585	URI Manipulation to strip the 1 from inbound ANI is no longer working since our SBC rebooted on Friday
AURORA-1586	Calls blocked by "Max Concurrent Audio Session" erroneously reached
AURORA-1588	Inconsistencies in GUI terminology

AURORA-1598	UPDATE issue: 1st UPDATE has target IP in To header, subsequent UPDATEs have SBC B1 IP in To header
AURORA-1602	Typo in the Dashboard GUI
AURORA-1611	Win Flare (SBC) is failed to escalate P2P call with 1XC to Conf
AURORA-1615	Unique engine ID for SNMPv3
AURORA-1618	Protocol Discriminator Selection shows default value i.e. 0x00 in the drop-down while selected value is 0x04
AURORA-1621	Ssyndi restarts when moderator tries to mute a participant as part of meet me conference
AURORA-1629	SBC does not transfer BYE message when Emergency Call ends
AURORA-1640	RTCP: RTCP packet sent from a wrong interface for a inter core call
AURORA-1642	When downgrade is done from 6.2.1 Q02 to 6.2.0Q58 and on subsequent upgrade to 6.2.0Q59 TLS certificate and key folders get deleted
AURORA-1645	SBC-E uses wrong R-URI in a SUBSCRIBE message
AURORA-1646	SBC is not passing on a Via Header correctly
AURORA-1651	Trigger - After upgrade to Q60 completes message "At least one device must be selected"
AURORA-1655	Content-type Header missing in 200OK during ICR Call flow when doing delayed offer
AURORA-1661	Attended Transfer is not working when SIP End Managed Transfer is turned On.
AURORA-1664	Domain DoS screen on GUI doesn't allow input for max concurrent sessions for Remote User Traffic Type
AURORA-1665	/usr/bin/python /etc/init.d/ipcs-init all script takes over HA port 1950 causing HA transport to shutdown
AURORA-1671	Management Interface(M1) is not taking effect and wrong interface detection on Dell 210 II platform with 6.2.1u installer
AURORA-1678	Blacklist URI Group is not able to Add in Security Rules
AURORA-1685	Add validations on PPM transactions - issue detected during customer TPG vulnerability scan failure

List of known issues

Key	Summary
AURORA-1421	Processes went down on EMS (HA Pair) after restoring the snapshot(Backup/Restore)
AURORA-1442	Trigger: Unable to process calls for 2-3 minutes during SBC HA upgrade to 6.2Q50
AURORA-1494	vi: The call is dropped when CMES_1_96x1 answers call from PSTN simulator user over MM and SBC.
AURORA-1498	Israel change the Daylight saving time schedule, request to patch the time zone pkg
AURORA-1500	Digicel Haiti had SSYNDI die and possible database corruption at same time.
AURORA-1537	Trigger: SBC Responding to INVITE with Server Internal Error resulting in call not delivered
AURORA-1540	Trigger:200OK Response to INVITE Lost through SBC b2b2b after ASM Deny New Service
AURORA-1556	dynamic flows aren't cleared after MU test
AURORA-1573	Trigger: HA-SBC 1st fail over after long idle or low traffic period causes significant loss of CTI
AURORA-1649	Scrubber incidents are being detected for valid call-related messages
AURORA-1673	Call transfer Failed with Cisco Trunk
AURORA-1687	Domain Dos incidents for Remote and Trunk Traffic are detected prematurely
AURORA-1716	SBC env': Video image freeze after 5 min' and Audio RTP stops after 16 min', of active Video call sessions
AURORA-1720	SIPERA does not forward 200 OK message related to a reInvite procedure
AURORA-1734	EMS processes fail to start on Restore action
AURORA-1740	traceSBC doesn't function correctly when its run during traffic
AURORA-1741	Media Anomaly detected (MAD) for IP Office one-x mobile remote workers Voice Mail (VM)
AURORA-1742	Call cannot be terminated
AURORA-1744	Re-INVITE handling transmits ACK
AURORA-1745	SSYNDI restarted with core dump due to out of memory while running UDP Trunk soak at 80cps and 83sec hold time with 6640 sessions
AURORA-1747	SSYNDI process outage in SBC during processing of RTCP Subtype 5 Traceroute information for Prognosis support
AURORA-1756	Cli is prompting for the challenge response for the ASG users even though the ASG authentication is disable (only after installation)
AURORA-1759	Sip parser fails to reassemble complete sip message causing transfer to Fail.
AURORA-1760	Subscription denied
AURORA-1761	Statistics : total calls counter is misleading
AURORA-1767	Lync Certification : RTCP generation in SBC when SIP trunk does not support RTCP generation
AURORA-1768	Lync Certification : Reliable Early Media (PRACK) : Sending/Receiving Pack and supported : 100 rel in case of Trunk provider do not support them
AURORA-1769	Lync Certification: support for UCSEC to handle Ptime=40 on Lync Side while SIP trunk supports only Ptime=20
AURORA-1770	SSYNDI restarted with Core during traffic test with HA failover
AURORA-1771	SSYNDI Memory increased to 1.7MB during failovers with traffic tests.
AURORA-1772	ASG authentication file installed, but ASG query fails
AURORA-1843	Flare Windows video srtp call denied

Known workarounds to apply

Multi SM configuration remote worker: Remote worker REGISTRATION are denied and calls are also denied when Time of Day is applied (AURORA-1227)

Time of day configuration should not be used for remote worker.

Remote Phones are sending "UNENCRYPTED_SRTCP" when Media anchoring in disabled, which results in call failure (AURORA-607)

Media anti-tromboning is not supported for this release. The workaround is to not disable media anchoring.

Call transfer failed with REFER-Handling, when transfer from call server to trunk server (AURORA-867)

The following describes SBC behavior while handling REFER message.

- REFER message is handled by SBC when REFER handling is enabled for server to which the REFER is being sent.
- While the REFER message is handled by SBC, an INVITE message is generated by SBC and sent to the transfer target as if the INVITE was received by transferee.
- SBC routes the generated INVITE message to appropriate server directly.

For above mentioned behavior to work there are certain configurations required.

- Proper routing entry in routing profile of the server to which REFER message is handled so that the INVITE generated is routed to the proper server.
- Proper server flow for the server to which INVITE generated is sent.

AST-2 transfer for trunks (AURORA-1673)

In this release AST-2 transfer is supported only for remote workers. For trunks it is not supported because of the known Communication Manager issue (defsw130462 and defsw130568).

- **defsw130462** -- Interaction of Dial-plan-transparency and AST2
- **defsw130568** -- AST2 xfer fails with team button and interaction

In the case of the trunk deployment, configure Communication Manager to use only AST-1.

Multi SM configuration trunking

In the current 6.2 load, multiple Session Managers support is:

- Two Session Managers for the SIP trunking operation.
- Two Session Managers (one primary and one secondary) for remote worker registration.

Avaya SBC-E delivering both Remote Worker and SIP trunk service (Aurora-633, AURORA 631)

If the Avaya SBC-E should deliver SIP trunk service, it needs to be administered as a trusted server at the Session Manager and System Manager level. For remote worker deployment, the SIP Entity Link must not be configured. Configuring Session Manager entity links for remote workers results in major Authentication issues. Remote and Trunk residing in same deployment requires two call server side interface IP address where one IP address corresponds for trunk service with SIP entity link and other internal interface corresponds for remote worker deployment which must not be configured as SIP entity. This resolves the origination treatment and incorrect login issues. Similarly, on the external side, it one IP address is required for remote worker and one IP address is required for trunks.

Another workaround is to use two different Avaya SBC-E systems or to administer different ports on Session Manager for the trunk service and for the remote worker service.

SM SIP firewall configuration

Session Manager SIP firewall rate limits the number SIP messages from an IP Address. These limits are based on the traffic from a single endpoint. To avoid rate limiting of the messages from SBC-E:

- SBC-E IP address should be whitelisted in Session Manager SIP firewall.
- Session Manager SIP firewall function should be disabled for remote worker solution.

Time needs to be synchronized during install between EMS and Avaya SBC-Es for any separate EMS based deployments

The installation fails if the time is not in synch between the EMS and Avaya SBC-E in separate box or high availability (HA) deployment. The time/NTP needs to be configured during the initial installation to ensure all Avaya SBC-E boxes and the respective EMS are synchronized.

Capneg configuration (AURORA-1094)

When configuration is enabled, media rules should have at least two lines: one with RTP and one with SRTP; otherwise the CapNeg offer will not happen.

Scrubber: false positives (AURORA-1263, AURORA-1268)

Some of the scrubber rules detected for legitimate call flow. Following is the list of the rules and the workarounds:

- Rule 80 - detects anomaly for a conference call between 9640 endpoints as part of contact header in Update message.

  Workaround: Disable rule 80.

- Rules 114, 116, 118 configured to Drop_Header. Drop_Header for mandatory headers like To, From and Call-id does not work.

  Workaround: Do not configure Drop_Header.

Call server REGISTER to trunk server then calls from trunk fail (AURORA-1370)

There is an issue on INVITE message routing from trunk to call server; Trunk Server is adding SBC-E subscriber id on the INVITE Request Line.

Workaround: Add the following SigMa script to trunk server configuration.

```
within session "ALL"
{
  act on request where %DIRECTION="INBOUND" and
%ENTRY_POINT="AFTER_NETWORK"
  {
        if(exists(%HEADERS["Request_Line"][1].PARAMS["subid_ipcs"]))
then
        {
            remove(%HEADERS["Request_Line"][1].PARAMS["subid_ipcs"]);
        }
   }
}
```

For Fresh Install/ Upgrade-Rollback or EMS Replication processes do not come up unless Application Restart is done (AURORA-1122)

Sometimes after a fresh install or upgrade of SBC-E or EMS applications will not start automatically.

Workaround: Make sure that openvpn between SBC and EMS is up and perform a manual application restart.

Problem changing application relay administration (AURORA-1188)

SBC-E cannot convert TCP to TLS or TLS to TCP using application relay. It is not recommended for conversion between TCP to TLS or vice versa in SBC-E.

Primary goes down and does not come up if you start GUI Packet Capture and do failover (Kill SSYNDI, GUI Reboot, GUI Application Restart, Shutdown) (AURORA-1208)

Workaround: Manually restart the failed SBC-E.

Processes went down on EMS (HA Pair) after restoring the snapshot (AURORA-1421)

Workaround: Restart EMS and SBC-E after restoring the snapshot.

Roll back failed to 4.0.5.Q20rc6 (AURORA-1416)

Rollback to an rc load is not supported.

Workaround: Upgrade 4.0.5.Q20rc6 to 4.0.5.Q21 and then upgrade to 6.2.0.Q58. If there is any issue, rollback to 4.0.5.Q21 which is same as 4.0.5.Q20rc6.

Processes went down on EMS (HA Pair) after restoring the snapshot (Backup/Restore) (AURORA-1421)

This issue occurs when the GUI caches the network passphrase at startup as a static final constant.

Workaround: Manually restart the GUI to force the GUI to pull the new password. Then, restart the application.

Trigger: Unable to process calls for 2-3 minutes during SBC HA upgrade to 6.2Q50 (AURORA-1442)

During the upgrade, the SBC service may be down for few minutes.

Workaround: Perform upgrade only during a maintenance window.

traceSBC doesn't function correctly when its run during traffic (AURORA-1740)

Running traceSBC tool might impact the Avaya SBC-E performance.

Workaround: Avoid using traceSBC during the busy hour.

Media Anomaly detected (MAD) for IP Office one-x mobile remote workers Voice Mail (VM) (1741)

Ignore all the MAD incidences reported. In this release, MAD is not supported.

CLI is prompting for the challenge response for the ASG users even though the ASG authentication is disable (only after installation) (AURORA-1756)

In the case of EMS or single box first login after disabling the ASG authentication may fail, but subsequent attempts will succeed.

ASG authentication file installed, but ASG query fails (AURORA-1772)

Sometimes pushing the installed ASG file from EMS to SBC may fail. In this case ASG authentication from SBC will fail.

Workaround: Manually perform the sync from EMS CLI/GUI or SBC CLI to fix this issue.

Total call counter is misleading (Aurora-1761)

In a remote worker solution, if One-X Mobile SIP iOS endpoints are used, the total number of calls reported in the Statistics is erroneous.

Workaround:

1. Create a subscriber flow for this endpoint type.
2. Check the total number of calls reported in the statistics for this type.
3. Subtract this number from the total number of calls to get a correct number for all endpoint types except One-X Mobile SIP iOS.

SRTCP for video (Aurora-1843)

When SRTP is configured for video, make sure to disable “Encrypted RTCP”, usually “Encrypted RTCP” is enabled by default.