Avaya Aura® SIP Third Party Interoperability Strategy

Version 2.0 Dated 9 April 2012

Introduction

The Avaya Aura® solution gives new meaning to how enterprise Unified Communications delivers business value by connecting the right business applications with the right user agnostic of device, platform and location. A chief advantage of the Avaya Aura solution is the ability to deliver the right features to the right users independent of network or endpoint device. With the Avaya Aura solution, system architects and planners have the advantage to choose the endpoint, gateway or other network component that satisfies the user's needs and delivers *"fit for purpose"* services across an entire enterprise.

The Avaya Aura solution includes a complete portfolio of communications components including endpoints, applications, servers, gateways, and other devices needed for comprehensive enterprise solution. However, the Avaya Aura solution has been specifically engineered for tight interoperability with other vendor's standards compliant devices. This open standards approach enables greater flexibility for customers that either require third party equipment or seek to maximize previous investments. Moreover, the Avaya Aura solution embraces partner, 3rd party, and independently-developed application integration via SIP to the core.

Because the Avaya Aura solution is based on IETF SIP standards, interoperability with third party equipment is focused on (but not limited to) compliance with these standards. This document emphasizes how the Avaya Aura solution interoperates with third party equipment (Cisco, Siemens, etc., as well as members of the Avaya DevConnect program) is accomplished based on SIP standards, and the degree to which various levels of interoperability are supported by Avaya Client Services.

Avaya Aura Standards Compliance

Avaya is committed to compliance with well accepted industry standards. Standards compliance yields the following customer benefits:

1. Avaya protects customer investments made with third party vendors by allowing the use of third party equipment alongside the Avaya Aura solution

2. Standards provide a blueprint for interoperability, providing the interface where compatibility between vendors is defined

3. Best in class devices can be chosen from each vendor allowing the highest quality overall solutions that include the Avaya Aura solution set

Avaya is so committed to standards compliance that in the event a customer interoperability issue critical to a customer's business is determined by Avaya to be a violation of the applicable supported SIP standard, Avaya will modify the Avaya Aura product to meet compliance with the SIP standard.

The applicable SIP standards for the Avaya Aura products are listed below. The Avaya Aura product documentation will provide details on deviations or changes to standards when applicable.

Note: The following standard list is not comprehensive; many standards apply in many configurations and functions, but not all the listed standards apply for all situations and all Avaya Aura components. Depending on the configuration and purpose, The Avaya Aura solution may only support portions of the standards listed below.

RFC 0791	Internet Protocol
RFC 0792	Internet Control Message Protocol
RFC 0793	Transmission Control Protocol
RFC 0951	Bootstrap Protocol
RFC 1034	Domain names - concepts and facilities
RFC 1035	Domain names - implementation and specification
RFC 2046	MIME Part II – Media Types
RFC 2198	RTP Payload for Redundant Audio Data [packet redundancy]
RFC 2246	Transport Layer Security – TLS
RFC 2327	Session Description Protocol
RFC 2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC 2401	IPSec
RFC 2412	IPSec
RFC 2543	SIPv2
RFC 2782	DNS RR for specifying the location of services (DNS SRV)
RFC 2833	Telephone Events (DTMF)
RFC 2906	SIP Info Method
RFC 3087	Use of URIs for Services
RFC 3164	Syslog Logging
RFC 3261	Session Initiation Protocol
RFC 3262	PRACK
RFC 3263	SIP: Locating SIP Servers
RFC 3264	An Offer/Answer Model with Session Description Protocol
RFC 3265	SIP-Specific Event Notification
RFC 3311	The SIP UPDATE Method
RFC 3323	Privacy
RFC 3324	Short Term Requirements for Network Asserted Identity
RFC 3325	Private Extensions to SIP for Asserted Identity within Trusted Networks
RFC 3327	SIP Extension Header Field for Registering Non-Adjacent Contacts
RFC 3326	Reason
RFC 3420	Message/SIPfrag
RFC 3425	P-Asserted
RFC 3428	Instant Messaging
RFC 3515	The SIP REFER Method

RFC 3578	Overlap Signaling
RFC 3581	Rport
RFC 3605	RTCP attribute in SDP
RFC 3665	SIP Basic Call Flow Examples
RFC 3666	PSTN Call Flows
RFC 3680	Registration Event Package
RFC 3711	SRTP
RFC 3725	3PCC
RFC 3840	Callee Capabilities
RFC 3841	Caller Prefs
RFC 3842	A Message Summary and Message Waiting Indication Event Package for SIP
RFC 3856	A Presence Event Package for the Session Initiation Protocol (SIP)
RFC 3857	A Watcher Information Event Template-Package for SIP
RFC 3858	An Extensible Markup Language (XML) Based Format for Watcher Information
RFC 3860	Common Profile for Instant Messaging (CPIM)
RFC 3863	Presence Information Data Format (PIDF)
RFC 3891	SIP "Replaces" Header
RFC 3892	Referred-By
RFC 3903	PUBLISH
RFC 3911	Join
RFC 3968	IANA Header Field Parameter Registry
RFC 3969	IANA URI Parameter Registry
RFC 3986	URI Generic Syntax
RFC 4032	Update to SIP Preconditions Framework
RFC 4028	Session Timers in SIP
RFC 4083	3GPP IMS General
RFC 4235	An INVITE-Initiated Dialog Event Package
RFC 4244	Request History Information
RFC 4353	Conferencing – isfocus
RFC 4475	SIP Torture Tests
RFC 4538	Authorization through Dialog Identification
RFC 4566	Session Description Protocol
RFC 4568	Security Descriptions for Media Streams
RFC 4733	Telephone Events (DTMF)
RFC 4734	Definition for Events for Modem Fax and Text
RFC 5626	SIP Outbound
RFC 5853	Session Border Controller for Enterprise

Avaya Aura Solution Verification & Support Processes

The Avaya DevConnect program accepts third party endpoint requests for testing and performing comprehensive, professional test services, under the aegis of the DevConnect Compliance Testing process. A device or solution is considered "supported" if it has undergone rigorous interoperability testing through the Avaya DevConnect program, the Avaya Solution Integration and Test Lab, or by Avaya Professional Services personnel as part of a professional services engagement, and detailed Application Note(s) produced documenting the exact test setup and configuration (including software release versions) for both the Avaya and third-party product(s).

In the event an Avaya customer utilizes and experiences issues with a third-party SIP device or an application that has been previously tested by Avaya, Avaya Client Services will provide support to a customer covered by an Avaya maintenance contract on the Avaya Aura solution by doing the following:

1. Validate that the Avaya components are configured correctly.
2. Utilizing the published Application Notes, make a "best effort" to validate the parameters identified within the notes.
3. If the third party SIP device or application is not performing as to the customer expectations and items 1 and 2 have been validated, Avaya Services will refer the customer back to the manufacturer, who may then engage the Avaya DevConnect program for additional lab-based issue re-creation and troubleshooting.

As the DevConnect organization continues to perform interoperability testing for third party SIP devices and publish additional Application Notes, Avaya will continue with support as noted above.

Support for all other third party SIP devices and applications not validated through Avaya DevConnect are the sole responsibility of the end-user customer.

Customers can pursue any of the following options to achieve support for their preferred third-party SIP device or application, with the supported third party phones:

- Request the third-party vendor to join the Avaya DevConnect program (www.avaya.com/devconnect) and complete compliance testing for interoperability.
- Contract with the Avaya Professional Services to perform the integration on a time and materials basis.

Should an Avaya customer utilize SIP endpoints that have no Avaya or DevConnect Application Notes or any other formal supporting relationship with Avaya and in the event of a customer issue, Avaya Client Services will support a customer covered by an Avaya maintenance contract on the Avaya Aura solution by doing the following:

1. Validate that the Avaya components are configured correctly.
2. If the third party SIP device is not performing as to the customer expectations and item 1 has been validated, Avaya Services will refer the customer back to the manufacturer.

Avaya and DevConnect Application Notes may be found on the Avaya Support Portal (www.avaya.com/support) under *Application & Technical Notes*, based on the target Avaya Platform (i.e. Avaya Aura® Session Manager). :

Information on the Avaya DevConnect program is located at http://www.avaya.com/devconnect.

SIP Terminals

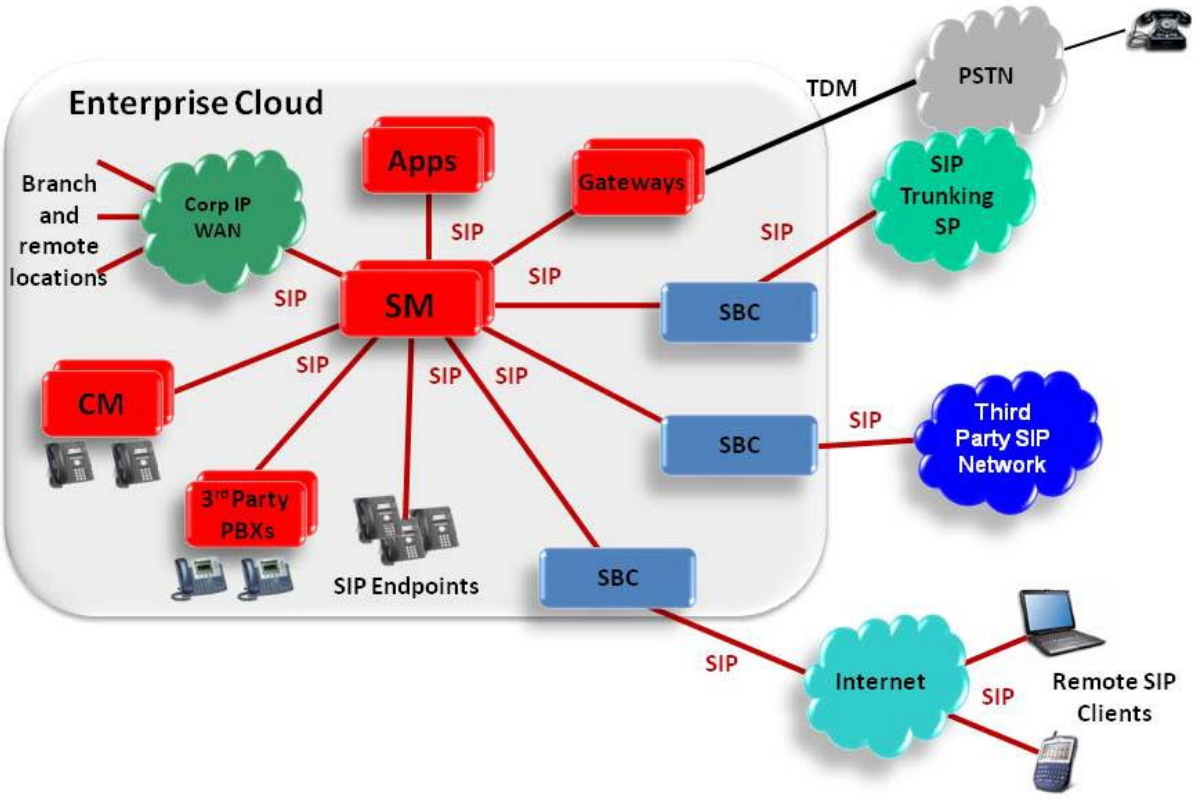
A major class of SIP devices critical to the Avaya Aura solution SIP interoperability is the class of end user devices operated directly by communications users – SIP terminals. To accommodate the general needs and expectations of Avaya Aura solution customers, Avaya has defined a core set of services (telephony features) verified with every end user endpoint device. Testing with third party endpoints via the DevConnect program or other Avaya Professional Services engagements will include the following:

- Basic incoming call
- Basic outgoing call
- Multiple line Appearances
- Hold, Un-hold
- Conference – 3 Party
- Transfer
- Mute
- Forward
- Music on hold
- Called and Caller ID and display
- Redial
- DTMF Tone sending
- Call Log
- Coverage to Voicemail
- Message Waiting Indication (MWI)
- Feature Access Codes (FAC)
- Feature Named Extensions (FNE)

The Application Note for each endpoint will describe the test results for these and any additional tests the vendor conducted with DevConnect. Unless specifically noted as successfully tested, any configuration, feature, or capability should be assumed to be un-supported.

Session Border Controllers

A second class of SIP devices of high interest is the Session Border Controller (SBC). The SBC plays an important role in the Avaya Aura solution architecture and is shown in the following figure.



The SBC provides the following critical enterprise functions:

- Topology hiding and NATing.
  - With an SBC, the address of the SBC is exposed through the corporate firewall for SIP signaling and RTP streams.
  - Without an SBC, the addresses of SIP phones, SIP gateways, PBXs, and applications that receive RTP streams inside the customer network must be made externally addressable.
- Security
  - SBCs provide denial of service and distributed denial of service protection from un-trusted networks. Some possible un-trusted networks shown above are Service Provider networks, the Internet, and third party company networks.
  - SBCs dynamically open and close the media ports as needed for SIP communications across the boundary between the trusted and un-trusted networks. This prevents firewall designs from allowing a range of unused RTP ports to be open, allowing a security "hole" at the network boundary.

  - SBCs provide SIP firewall and deep packet inspection to prevent Trojan horse, malformed packet, and other attacks on the enterprise network.
- Demarcation
  - The SBC represents a defined point in the network to determine where problems originate – either inside or outside the customer's network.
- Anchoring Media
  - SBCs prevent media changes within the enterprise from being "seen" by the external or un-trusted networks.
  - SBCs can reduce or eliminate take-back-transfer charges
  - SBC's provide codec conversion which adapts enterprise applications to SP codec requirements and can reduce enterprise network bandwidth usage.
- Flexibility
  - Without an enterprise SBC, configuration changes may need to be done by the Service Provider (SP) SBC. The service provider's network operations processes preclude rapid and frequent changes to the SPSBC platform configuration – primarily for stability reasons. Most service providers only offer one enterprise-facing configuration and will not change it.
  - By installing an enterprise SBC, the customer's specific communication requirements can be fully addressed, insulating the service provider's SBC from any changes. This means that the specific business needs of the customer can be met in a quick and easy way.

SBCs are critical to the security and successful operation of an Avaya Aura solution enterprise SIP network. As a result the relationship between the Avaya Aura solution and the SBC is tightly integrated. To ensure its success, Avaya has developed special rules for the deployment and support of SBCs into the Avaya Aura solution.

1. **Avaya fully supports the Avaya Session Border Controller for Enterprise and Advanced for Enterprise (SBCE/AE) for use with Avaya Aura solution configurations.**
   - Avaya Client Services will support configurations with these supported SBCs and the Avaya Aura solution.
   - If a customer interoperability issue critical to a customer's business is determined by Avaya to be a problem with the Avaya SBC or Avaya Aura equipment, Avaya will modify the Avaya SBCE/AE and/or Avaya Aura product to address the issue.

2. **Avaya supports SBCs other than Avaya SBCE/AE through the Avaya DevConnect Program. HOWEVER:**
   - Due in part to the number of interactions and technical complexity of the interface, Avaya undertakes significant efforts to test the Avaya SBCE/AE with the Avaya Aura solution While DevConnect Compliance Testing of third party SBCs is also thorough, its scope is limited in contrast

to the comprehensive internal Avaya product testing, and does not include performance, scalability, reliability or serviceability elements, nor does it ensure full, functional testing.

- Support provided by Avaya Client Services of the Avaya Aura solution interface operation with any other SBC is predicated on successful completion of DevConnect Compliance Testing, and is limited to triage and troubleshooting based on the availability of specific DevConnect Application Notes for the tested/deployed configuration.
- In contrast to the thousands of hours of interoperability, performance testing, longevity operation, and feature verification with the Avaya SBCE/AE, Avaya may not have experience or "soak time" logged in any Avaya laboratory with any other SBC. .
- Avaya cannot commit to modifying an Avaya Aura product to fix any customer interoperability issue with an untested SBC. Avaya will only consider modifying Avaya Aura products to address interoperability issues once it has been shown, via DevConnect testing, that the Avaya Aura solution is acting in a manner inconsistent with IETF SIP RFC's as listed above.
- Avaya Client Services can use the extensive tools resident in the Avaya software (e.g. Avaya Aura Session Manager, Communication Manager, Communication Server 1000, etc.) to examine the SIP message exchanges from Avaya Aura solution to the SBC. If this exercise requires analyzing unsupported SBCs or interactions with unsupported SBCs and it is determined Avaya's equipment is not at fault, then the services performed would be billable at Avaya's applicable per-incident rates.

3. **Avaya fully supports the Avaya SBCE/AE for use with Service Provider SIP offerings:**
   - Avaya Client Services will contract maintenance services and support configurations with the Avaya SBCE/AE and the Service Provider.
   - Support for a Service Provider offering is contingent on successful testing of the service with the enterprise Avaya SBCE/AE. The Avaya SBCE/AE should be verified if the Service Provider SIP offering is to be implemented with a choice of either enterprise SBC.
   - If a customer interoperability issue critical to a customer's business is determined by Avaya to be a problem with the Avaya equipment, Avaya will modify the product to address the issue.

4. **Avaya cannot certify or guarantee operation of the Avaya Aura solution with any Service Provider SIP trunking offer using an untested enterprise SBC.**
   - The degree of testing required for certification is high, as described in item 2 above. Avaya will not assume any responsibility for interactions between a third party SBC and a third party Service Provider SIP trunk.
   - Avaya cannot technically support a configuration as complex as the SBC-Avaya Aura solution interface without significant investment and experience.

5. **Avaya cannot certify or guarantee operation of the Avaya Aura Solution with any Service Provider SIP trunking offer without the implementation of an enterprise SBC.**
   - It is Avaya's position that Service Provider integration without an enterprise SBC is inherently un-secure and the Avaya Aura solution by itself without a supported enterprise SBC cannot guarantee the security of the enterprise.
   - Avaya Client Services and Avaya product teams have little or no experience with this configuration and cannot support it to the satisfaction of our customer base.

More information

For more information on Avaya Aura, please access the Partner Portal home page and link to Solutions and Products from the left navigation bar. From the Central navigation select Products A-Z under Products, Services and Solutions and then select Avaya Aura Communication Manager, Avaya Aura Session Manager, Avaya Aura System Manager, Avaya Session Border Controller Advanced for Enterprise and Avaya Session Border Controller for Enterprise.