



Avaya Aura[®] Application Enablement Services R6.2 Server and Client Release Notes

Issue 1.4
April 2013

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Release 6.2 and describes important notes and known issues.

WHAT'S NEW IN AE SERVICES 6.2?

- Cell Phone Recording
- Communication Manager Software Duplication
- Support for Machine Preserving High Availability
- Historical Metric Data Collector enhancements
- Telephony Services Application Programming Interface (TSAPI) enhancements
- Enhancements for Agile Communication Environment[™] and Avaya Aura[®] Contact Center
- Adjunct Switch Applications Interface (ASAI) enhancements
- Avaya Aura[®] AE Services 6.2 Virtualization Enablement (VE) vAppliance for deployment on VMware ESXi 5.0 infrastructures

For additional information, please reference the Avaya Aura[®] Application Enablement Services Overview at <https://downloads.avaya.com/css/P8/documents/100164154>

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura [®] Application Enablement Services 6.2 Software Only 32-bit and 64-bit in 32-bit compatibility mode - 700503207	swonly-r6-2-0-18-20120529.iso
Avaya Aura [®] Application Enablement Services 6.2 Hardware Bundled Upgrade for S8510 - 700503206	bundled-r6-2-0-18-20120529.iso
Avaya Aura [®] Application Enablement Services 6.2 on System Platform - 700503208	aes-r6-2-0-18.iso
System Platform Service Pack R6.2.1	vsp-6.2.1.0.9.iso
Avaya Aura [®] AE Services 6.2 Virtualization Enablement (VE) vAppliance	AES-6.2.0.18.20120529-e50-07.ova
Avaya Aura [®] Application Enablement Services 6.2 CVLAN Client Linux 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-linux-6.2-257.i386.rpm
Avaya Aura [®] Application Enablement Services 6.2 CVLAN Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-win32-6.2-257.zip

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 6.2 TSAPI Client Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-linux-6.2-257.i386.rpm
Avaya Aura® Application Enablement Services 6.2 TSAPI Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-win32-6.2-257.zip
Avaya Aura® Application Enablement Services 6.2 TSAPI SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-linux-6.2-257.i386.rpm
Avaya Aura® Application Enablement Services 6.2 TSAPI SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-win32-6.2-257.zip
Avaya Aura® Application Enablement Services 6.2 JTAPI SDK	jtapi-sdk-6.2.0.54.zip
Avaya Aura® Application Enablement Services 6.2 Web Service - System Management SDK	smssvc-sdk-6.2.0.69.zip
Avaya Aura® Application Enablement Services 6.2 DMCC .Net SDK 32-bit and 64-bit in 32-bit compatibility mode	dmcc-dotnet-sdk-6.2.0.29.zip
Avaya Aura® Application Enablement Services 6.2 Web Services - Telephony SDK 32-bit and 64-bit in 32-bit compatibility mode	telsvc-sdk-6.2.0.69.zip
Avaya Aura® Application Enablement Services 6.2 DMCC XML SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapixml-sdk-6.2.0.69.zip
Avaya Aura® Application Enablement Services 6.2 DMCC Java SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapijava-sdk-6.2.0.69.zip
Avaya Aura® Application Enablement Services Product Management Information Bases (MIBs)	aesvcs-product-mibs-6.2.0.69.zip
Standard MIBs	standard-mibs-6.2.0.69.zip

IMPORTANT NOTES

- AE Services 6.2 supports Red Hat Enterprise Linux 5.0 Update 7 for 32-bit x86
- AE Services 6.2 is compatible with the following Bundled Server: Dell 1950 (S8510)
- AE Services 6.2 on System Platform is compatible with the following Servers:
 - IBM x3550 M2 (S8800)
 - Dell R610 (4GB RAM, H200 RAID Controller, 2x146 GB HDDs)
 - Dell R610 (6GB RAM, H700 RAID Controller, 2x300 GB HDDs)
 - HP DL360G7 (12GB RAM, P410i RAID Controller, 2x300GB HDDs)
- AE Services 6.2 on System Platform is compatible with the following versions of System Platform:
 - System Platform R6.2.1 - **Do not install AE Services on System Platform R6.2.** AE Services is not certified with System Platform R6.2. AE Services is certified against System Platform R6.2.1 service pack (July 2012). AE Services systems should be upgraded to System Platform R6.2.1 service pack before the AE Services R6.2 template is upgraded. There is an interaction between System Platform R6.2 and certain Dell R610s that can cause the system to crash under high I/O.
 - System Platform R6.2.2.09001.0
- AE Services 6.2 is compatible with the following Communication Manager Releases and Platforms:
 - Communication Manager 5.2.x
 - Communication Manager 6.0.x
 - Communication Manager 6.2 SP2
- Communication Manager 6.2 is compatible with the following AE Services Releases:
 - AE Services 5.2.4
 - AE Services 6.1.2
 - AE Services 6.2

Communication Manager 6.2 Service Pack 1 is not supported.

Avaya SIP Endpoints Supported by AE Services

Endpoint	Administered as	Endpoint Firmware	AE Services Release	CM/ASM Pair		General Telephony	Agent Features
				CM- ES Version	ASM Version		
9620	9620SIP	2.6 SP6	6.2	6.2	6.2	yes	no
9640	9640SIP	2.6 SP6	6.2	6.2	6.2	yes	no
9640G	9640SIP	2.6 SP6	6.2	6.2	6.2	yes	no
9630G	9630SIP	2.6 SP6	6.2	6.2	6.2	yes	no
9650	9600SIP	2.6 SP4	6.2	6.2	6.2	yes	no
9608	9608SIPCC	6.2	6.2	6.2	6.2	yes	Yes
9611	9611SIPCC	6.2	6.2	6.2	6.2	yes	Yes
9621	9621SIPCC	6.2	6.2	6.2	6.2	yes	Yes
9641	9641SIPCC	6.2	6.2	6.2	6.2	yes	Yes

Endpoint	Administered as	Endpoint Firmware	AE Services Release	CM/SES Pair		General Telephony	Agent Features
				CM Version	SES Version		
9620	9620SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9640	9640SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9640G	9640SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9630G	9600SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9650	9600SIP	2.6 SP4	6.1.x	6.0.1	6.1 SP2	yes	no
9608	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9611	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9621	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no
9641	9640SIP	6.0 SP1	6.1.x	6.0.1	6.1 SP2	yes	no

Note 1 - Agent Buttons Supported:

Agent Login/Logout
 After Call Work (ACW)
 Auxiliary (AUX) Work
 Auto-In/Manual-in
 Release
 Agent Event Package (16CC)

Release History:

Date	Server Build	Change(s)
03/2007	47-3	Release 4.0
06/2007	50-1	Release 4.0.1
12/2007	31-2	Release 4.1
04/2008	4.1.16	Release 4.1.1 JTAPI Client/SDK
05/2008	19-4	Release 4.2
08/2008	20-5	Service Pack R4.2.1
06/2009	31	Service Pack R4.2.2
09/2009	33	Service Pack R4.2.3
11/2009	98	Release 5.2
02/2010	103	Service Pack R5.2.1
06/2010	105	Service Pack R5.2.2
08/2010	35	Service Pack R4.2.4
02/2011	20	Release 6.1
03/2011	110	Service Pack R5.2.3
06/2011	30	Service Pack R6.1.1
10/2011	111	Avaya Aura® Application Enablement Services 5.2.3 Hardware Bundled Upgrade for S8510
10/2011	31	Avaya Aura® Application Enablement Services 6.1.1 Hardware Bundled Upgrade for S8510
03/2012	32	Service Pack R6.1.2
07/2012	18	Release 6.2
11/2012	18	Avaya Aura® AE Services 6.2 Virtualization Enablement (VE) vAppliance

KNOWN ISSUES AND WORKAROUNDS

- **AE Services on System Platform Template Upgrade Where the AE Services Server Uses a Dual NIC Configuration**

If the AE Services template is configured for a dual NIC, please execute the following steps in order to upgrade the AE Services on System Platform Offer template.

1. Document the AE Services template existing eth0 IP address, eth1 IP addresses, hostname, and netmask. This information can be obtained using the System Platform Management Console screen, “Server Management | Network Configuration”, in the section titled “Templates – AES”.
2. Backup the AE Services server data using the AE Services Management Console screen, “Maintenance | Server Data | Backup”.
3. Delete the current AE Services on System Platform Offer template using the System Platform Management Console screen, “Virtual Machine Management | Templates”.
4. Install the new AE Services on System Platform Offer template using the System Platform Management Console screen, “Virtual Machine Management | Templates”. During the install process, configure the network data using the information obtained in step 1.
5. Once the install successfully completes, restore the AE Services server data obtained in step 2 using the AE Services Management Console screen, “Maintenance | Server Data | Restore”.

- **File corruption can occur when the system experiences an ungraceful shutdown.**

The following steps should be taken to prevent an ungraceful shutdown: Do not disrupt the system power. An Uninterruptible Power Supply (UPS) or other type of uninterruptable power backup is a requirement with AE Services running on System Platform. See Chapter 2 of the Installing and Configuring Avaya Aura[®] System Platform product documentation on support.avaya.com.

- Sudden loss of power causes an ungraceful system shutdown which can lead to file system corruption. This includes pressing the power button or unplugging the server. See PSN 2987u for additional details.
- AE Services running on an S8800 Server can experience a non-maskable interrupt (NMI). This can cause an ungraceful shutdown. See PSN 2965u for additional details. Refer to PCN 1716B Supplement 1 for details on how to remediate this problem.

- **AE Services Session interaction with interchanges on duplicated Communication Manager media servers using the software duplication option**

Depending on the conditions under which a duplicated Communication Manager server pair utilizing software duplication interchange, AE Services sessions to that Communication Manager may be reset. All Java Telephony Application Programming Interface (JTAPI), TSAPI, CallVisor Local Area Network (CVLAN), and DEFINITY LAN Gateway (DLG) associations with that Communication Manager will be lost and will have to be recovered. The probability of a session being reset is directly proportional to the message rate between an AE Services server and Communication Manager when the interchange occurs, and is equally as likely with a spontaneous interchange (caused by a hard failure) as with a requested interchange (caused by, for instance, a craft request). This issue affects **all** AE Services releases.

Typically, the Link Resiliency feature introduced in AE Services 3.1 would allow AE Services sessions to survive such interchanges, and, with hardware duplication on Communication Manager, they still do. Starting with Communication Manager release 6.2, AE Services sessions will again survive controlled interchanges with software duplicated Communication Manager media servers (requires no change to AE Services release), but still will not survive spontaneous interchanges. Controlled interchanges are those in which the duplicated Communication Manager media servers are communicating with each other throughout the interchange, and covers the majority of interchanges that take place. Spontaneous interchanges occur when the physical linkage between the Communication Manager media servers is severed during the interchange process (typically caused by physical hardware failure on one of the media servers), and, as such, are not as prevalent as controlled interchanges.

- **Cannot get license version from WebLM Server**

If the error message “Cannot get license version from WebLM Server” is displayed on the “Maintenance | Server Data | Restore Database Configuration” screen after a restore, and a license file exists in the backup image, go to the “AE Services” screen to view the license information for each AE Service. If the license in the backup image is invalid, install the 6.X license file to resolve the issue. Be sure to uninstall any previous license files (i.e. 4.X or 5.X license) prior to installing the 6.X license file.

- **CVLAN Linux Client**

Before installing the CVLAN Linux client on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required:

openssl097a-0.9.7a-9.el5_4.2.i386.rpm.

This RPM may be available with the Red Hat Linux installation media and is also available for download at <http://rpm.pbone.net>.

- **CVLAN Services Does Not Display Online**

If there are no CVLAN links administered, the CVLAN Service will appear as "OFFLINE" on both the AE Services summary page and the Status summary page of the AE Services Management Console. The status will change to "ONLINE" after you administer at least one CVLAN link.

This is desirable behavior because it stops CVLAN from listening on a port that the customer is not using and stops that listening port from being reported as a risk on a security audit.

- **H.323 registration recovery fail after HA failover or AE Services restart**

An H.323 registration may not be recovered when Communication Manager fails over to either an ESS or LSP. This may occur if the registration was previously recovered through DMCC Service Recovery because of a System Platform HA failover or DMCC JVM restart.

- **Device Media Call Control (DMCC) will lose filter_multiple_switchhooks configuration after upgrading AE Services server software**

To have DMCC not filter out multiple switch-hook events, change the property 'com.avaya.mvcs.station.StationManager.filter_multiple_switchhooks' to 'false' in the /opt/mvap/conf/user-configuration.properties. This setting may reset to the default of 'true' during an AE Services upgrade. Verify the property value and reset it if required.

- **DMCC/TR87 can not properly track call made to Vector Directory Numbers (VDNs) or hunt-groups**

When a call reaches a VDN and is answered on the far end by an agent or the call reaches a hunt group, Office Communicator will create a phantom screen pop and any further transfers will result in new screen pops. This is similar behavior to when a call is alerting on one station and is answered immediately on a different station DMCC assumes it is a bridged station as there is no differentiation in behavior. Suppressing bridged call appearances for the station (or VDN) alleviates the issue unless the stations involved are SIP stations.

- **DLG Links**

DLG links may be OFFLINE after recovery from an abnormal shutdown.

- **DLG Service Does Not Display Online**

If there are no DLG links administered, the DLG Service will appear as "OFFLINE" on both the AE Services summary page and the Status summary page of the AE Services Management Console. The status will change to "ONLINE" after you administer at least one DLG link.

This is desirable behavior because it stops DLG from listening on a port that the customer is not using and stops that listening port from being reported as a risk on a security audit.

- **IPv6 issue with the DMCC Java SDK**

When attempting to connect to the AE Services server's IPv6 address using the DMCC Java SDK from Microsoft Windows, the user will see the following error message: "java.net.SocketException: Permission denied: connect"

Oracle is tracking this issue with IPv6 addresses for Java NIO channels on Windows. Currently there is no workaround. This issue will be addressed in a future release of Microsoft Windows.

- **The Microsoft Office Communicator client does not re-establish phone integration automatically when the AE Services server is restarted**

This is a known problem in OCS 2007 R2 that does not exist in LCS 2005. The following workaround is recommended:

1. The first attempt to make a call from an active OC after an AE Services restart will fail. Click the "retry" button to re-establish phone integration and also make the call.
2. Call events will not be reported to an active OC after an AE Services restart. To re-establish phone integration, sign-out of OC and then sign-in again.

- **OCS Integration and Microsoft Certificate Authorities (CA)**

When using Microsoft as the CA, Microsoft recommends using an Enterprise CA. The Enterprise CA template used to create the AE Services certificate must have the Enhanced Key Usage (EKU) field specified appropriately (Server and Client Auth or neither).

The LCS/OCS AE Services integration uses Mutual TLS (MTLS) to authenticate server-to-server SIP communication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA to prove the identity of each server to the other.

The server certificate used for MTLS on both servers must either not specify an Extended Key Usage (EKU) or specify an EKU for Server and Client Authorization. When the EKU is not specified the certificate is not restricted to a particular usage. However when the Key Usage field is specified and the EKU is specified as Server and Client Auth, the certificate can only be used by the server for mutual server and client based authentication purposes. If an EKU with only Server Auth is specified, in this scenario, the connecting server certificate will fail authentication and the MTLS connection will not be established.

The Standalone CA, which may also be used (but is not Microsoft recommended), does not provide configurable templates including some additional features and must adhere to the same certificate generation rules in regards to the EKU field.

Note that this statement doesn't preclude administrators from using non-Microsoft CAs (e.g. VeriSign).

- **Process to Change the Server Date and Time**

When the server time is changed by more than five minutes, several of the AE Services must be restarted. While these services will be restarted on their own, the following procedure is recommended for changing the AE Services Bundled or Software-Only server time:

1. Log into the AE Services Management Console.
2. Select "Maintenance | Service Controller".
3. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Stop".
4. When the confirmation screen is displayed, click on "Stop".
5. Select "Maintenance | Date Time/NTP Service", make the appropriate - changes on the web-page and click "Apply Changes".
6. When the confirmation screen is displayed, click on "Apply".
7. Select "Maintenance | Service Controller".
8. Set the check boxes for the ASAI Link Manager, CVLAN Service, DLG Service, Transport Layer Service and TSAPI Service, and then click on "Start".

For the AE Services on System Platform server, refer to the Administering Avaya Aura® System Platform document at

<https://downloads.avaya.com/css/P8/documents/100156656>

- **SIP Issues**

- When using 3rd party call control to make a call on a SIP endpoint to a VDN that has a vector step to collect digits after an announcement, the announcement will not be played and the digits entered will not be forwarded.
- When using 3rd party call control to make a call using a Communication Manger TAC (Trunk Access Code), the call will fail on a SIP phone if the Communication Manager does not have a TN2602AP board. Please note, it is

not common practice to use TAC dialing to access trunks. The Automated Alternative Routing (AAR) and Automated Route Selection (ARS) routing features are recommended methods of accessing trunks.

- If Communication Manager does not have a TN2602AP board, the media encryption on the SIP endpoint should be disabled. The SIP endpoint transport type must be set to TCP or UDP. If transport type is set to TLS, the 3rd party call control application may fail during transfer and conference.
- The Single Step Transfer Call service does not work reliably for SIP stations.
- Going off-hook on a SIP station followed by on-hook does not generate an INITIATED event.
- Using 3rd party call control when a call is made from a SIP station, the INITIATED event is slightly delayed as compared to other station types. Subsequent events are not delayed.
- ACD calls that are delivered to SIP endpoints are generating Alerting Event reports that do NOT contain the split/skill extension from the associated call.
- Avaya has observed intermittent problems with SIP endpoints in the 2.6SP4 and prior releases particularly with scenarios that result in Computer Telephony Intergration (CTI) requests that occur within a short time span of other CTI requests. It is currently not known when these issues will be completely addressed, but it is anticipated that future endpoint releases will address them fully.

- **Transport**

When a switch connection is deleted, the action is incomplete and any switch connections that are added may not function properly.

Workaround: Restart AE Services (or at least the Transport Layer Service) after deleting a switch connection.

- **TSAPI Linux Client**

Before installing the TSAPI Linux client on a Red Hat Linux ES v5.0 system, a separate installation of the following RPM may be required:

openssl097a-0.9.7a-9.el5_4.2.i386.rpm.

This RPM may be available with your Red Hat Linux installation media, and is also available for download at <http://rpm.pbone.net>.

- **Local WebLM Server Port Number**

If you have upgraded to AE Services 6.2 from an earlier release of AE Services, the local WebLM server may be configured to use port 443. Most AE Services customers will see improved WebLM performance if the port number is changed from 443 to 8443. Use this procedure to change the port number for the local WebLM server to 8443:

1. Use a web browser to log into the Application Enablement Services Management Console.
2. Select "Licensing | WebLM Server Address".
3. If the value of the WebLM IP Address is 127.0.0.1 and the value of the WebLM Port is 443, change the value of the WebLM Port to 8443 and click on "Apply Changes".
4. When the confirmation screen is displayed, click on "Apply".

After changing the WebLM Port, restart several of the AE Services:

1. Select "Maintenance | Service Controller".
2. Set the check boxes for "ASAI Link Manager", "CVLAN Service", "DLG Service", "Transport Layer Service", and "TSAPI Service", and click on "Restart Service".
3. When the confirmation screen is displayed, click on "Restart".

- **WebLM Session May Hang**

Performing one of the following actions on WebLM may hang the session.

1. Repeatedly uninstalling and installing licenses
2. Repeatedly refreshing the licensing page

The current session should be closed and a new session opened.

- **WebLM Enterprise Model – Using HTTPS**

Run this workaround if all three of the following conditions are true:

1. The master WebLM Server, which hosts the Enterprise License File (ELF), is not co-located with an AE Services server. The master WebLM server is either a standalone server or it is co-located in System Platform's CDOM.
2. The local WebLM servers are co-located with AE Services.
3. HTTPS is in use for communication between the master and local WebLM servers (for example, to push an Allocation License File (ALF) to the local WebLM server on AE Services).

The Enterprise Web Licensing WebLM patch, "importCertToWebLm.zip", is available on the AE Services CD/DVD ISO media. On the Hardware Bundled DVD, the patch is located in the "Patch" directory. On the Software Only CD, the patch is located in the root directory of the media. On the AE Services on System Platform DVD, the patch is located in the "licenses" directory.

1. Download [importCertToWebLm.zip](#) files to your EWL server.
2. Unzip the file.
3. Follow the directions in the README to install

KNOWN ISSUES AND WORKAROUNDS FOR AE SERVICES ON SYSTEM PLATFORM

System Platform issues affecting the AE Services on System Platform server are listed in the System Platform R6.2.1 release notes at

<https://downloads.avaya.com/css/P8/documents/100164142>

System Platform issues affecting the AE Services on System Platform server are listed in the System Platform R6.2.2 release notes at

<https://downloads.avaya.com/css/P8/documents/100168276>

RESOLVED ISSUES IN AE SERVICES RELEASE 6.2

• CVLAN CLIENT LIBRARIES AND SDKs

- Beginning with AE Services 6.2, the CVLAN Windows Client and SDK Setup program installs version 1.0.0d of the OpenSSL libraries instead of version 0.9.7g.

For installations where both the CVLAN Windows Client and the TSAPI Windows Client are installed on the same client host, Avaya recommends upgrading both the CVLAN Windows Client and the TSAPI Windows Client to AE Services 6.2 at the same time.

- Beginning with AE Services 6.2, if the user attempts to install the CVLAN Windows Client and SDK under “C:\Program Files” on 64-bit versions of Windows, the user is notified that the software will be installed under “C:\Program Files (x86)” instead.

• DMCC Service

- Improved the error log response in the case where a registered DMCC device in dependant mode against an IP phone is unregistered (not the DMCC device, just the physical phone) and getDisplay, setHookswitch and/or getButton info requests all generate the following response:

```
<?xml version="1.0" encoding="UTF-8"?><CSTAErrorCode  
xmlns="http://www.ecma-international.org/standards/ecma-  
323/csta/ed3"><unspecified /></CSTAErrorCode>
```

A TerminalUnregisteredEvent is now sent to the client application instead of the above CSTAErrorCode.

- A high percentage of AE Services H.323 endpoints were becoming unregistered during a failover. This was occurring due to the Primary Search Timer being set to 5 minutes on Communication Manager with ESS enabled. The Primary Search Timer value was recalculated for Communication Manager R6.2 to resolve the issue.
- Added support to detect a non-Microsoft LCS/OCS connection correctly.
- The AE Services shut down process now waits for the DMCC Service to shut down completely before reporting a successful result. This prevents the error condition where a new DMCC Service attempted to process messages destined for a previous instance.

- **.NET Service**

- When an Established or Delivered event contains an ACD Group, the .NET Service Provider was not delivering the ACD Group to the client. Added support to properly parse the ACD Group device ID.
- Provided a method (decodeDataToText) to convert user data in hex to plain text.
- Added .NET support for the termination element in the PlayMessage XML request and in the dashboard, added a checkbox to the Server Media tab under the Play button to control the termination option.
- Added support for the MonitorObjectData element called extension. This new element will be used to return the monitor called CallInformationEventsStartReponse as part of a GetMonitorList request.
- Added support for the RecordMessage option, “termination” in the .NET generated XML request. The Dashboard was modified to include a record message terminate checkbox on the Server Media tab in the Record Message section.
- Modified the ActiveX controller and javascript classes to properly handle a FailEvent and Transfer Event – reference the DevConnect Forum at https://devconnect.avaya.com/public/forum/d_forum_3.jsp?t=5217&f=23.
- Added a new Reconnect(...) method to allow the ability to recover an inactive or active session which still exists in DMCC, even if the request is issued from a new .NET Service Provider instance. The Dashboard was also modified to use this new method such that a session connection lost in one Dashboard instance can be recovered by another Dashboard instance.
- Added support for the media codec associated with the RecordMessage request.
- Added support for the gatekeeper address in the GetRegistrationStateResponse.
- Added support for the Service Link Status Changed event in the Phone/Physical Device monitor.
- Added support for the Snapshot Device private data item SnapshotDevicePrivateData which contains the param getStationStatus.
- Added support to Consultation Call for Consult Options.

- **Security**

The following Red Hat Linux security issues have been incorporated into Release 6.2:

1. [RHSA-2012:0107-01] Important: Kernel Security and Bug Fix Update - <https://rhn.redhat.com/errata/RHSA-2012-0107.html>
2. [RHSA-2011:0833-01] Important: Kernel Security and Bug Fix Update - <https://rhn.redhat.com/errata/RHSA-2011-0833.html>
3. [RHSA-2011:1245-01] Important: HTTPD Security Update - <https://rhn.redhat.com/errata/RHSA-2011-1245.html>
4. [RHSA-2011:0927-01] Important: Kernel Security and Bug Fix Update - <https://rhn.redhat.com/errata/RHSA-2011-0927.html>
5. [RHSA-2012:0007-01] Important: Kernel Security, Bug Fix, and Enhancement Update - <https://rhn.redhat.com/errata/RHSA-2012-0007.html>
6. [RHSA-2012:0104-01] Important: Libxml2 Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0104.html>
7. [RHSA-2012:0017-01] Important: Libxml2 Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0017.html>
8. [RHSA-2012:0094-01] Important: Freetype Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0094.html>
9. [RHSA-2011:1402-01] Important: Freetype Security Update - <https://rhn.redhat.com/errata/RHSA-2011-1402.html>
10. [RHSA-2011:0017-01] Important: Red Hat Enterprise Linux 5.6 Kernel Security and Bug Fix Update - <https://rhn.redhat.com/errata/RHSA-2011-0017.html>
11. [RHSA-2011:0472-01] Important: nss Security Update - <https://rhn.redhat.com/errata/RHSA-2011-0472.html>
12. [RHSA-2011:1349-01] Important: rpm Security Update - <https://rhn.redhat.com/errata/RHSA-2011-1349.html>
13. [RHSA-2011:0429-01] Important: Kernel Security and Bug Fix Update - <https://rhn.redhat.com/errata/RHSA-2011-0429.html>
14. [RHSA-2012:0324-01] Moderate: Libxml2 Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0324.html>
15. [RHSA-2012:0323-01] Moderate: HTTPD Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0323.html>
16. [RHSA-2012:0126-01] Moderate: glibc Security Update - <https://rhn.redhat.com/errata/RHSA-2012-0126.html>
17. [RHSA-2011:0492-01] Moderate: Python Security Update - <https://rhn.redhat.com/errata/RHSA-2011-0492.html>
18. [RHSA-2011:1797-01] Moderate: perl Security Update - <https://rhn.redhat.com/errata/RHSA-2011-1797.html>
19. [RHSA-2012:0307-03] Low: Util-Linux Security, Bug Fix, and Enhancement Update - <https://rhn.redhat.com/errata/RHSA-2012-0307.html>
20. [RHSA-2011:1005-01] Low: sysstat Security, Bug Fix, and Enhancement Update - <https://rhn.redhat.com/errata/RHSA-2011-1005.html>
21. [RHSA-2011:0844-01] Low: apr Security Update - <https://rhn.redhat.com/errata/RHSA-2011-0844.html>

- **TSAPI Client Libraries and SDKs**

- Beginning with AE Services 6.2, the TSAPI Service and private data libraries support private data version 10. Private data version 10 adds private data to the CSTA Logged On event and provides two new private data formatting functions:
 - attV10ConsultationCall() – allows an application to indicate the intended purpose (consult only, conference only, transfer only, or unrestricted) of a cstaConsultationCall() service request.
 - attV10QueryStationStatus() – reports a station's talk state and service state
- Beginning with AE Services 6.2, the TSAPI Windows Client Setup program installs version 1.0.0d of the OpenSSL libraries instead of version 0.9.7g.
- For installations where both the TSAPI Windows Client and the CVLAN Windows Client are installed on the same client host, Avaya recommends upgrading both the TSAPI Windows Client and the CVLAN Windows Client to AE Services 6.2 at the same time.
- Beginning with AE Services 6.2, the TSAPI Linux Client libraries (libcsta.so and libattpriv.so) only export symbols that are part of the TSAPI and Avaya private data Application Programming Interfaces (APIs). Previously, the TSAPI Linux Client libraries also exported local symbols and symbols from other third party libraries. This could cause linker errors or run-time issues for TSAPI applications that also used those other third party libraries.
- Beginning with AE Services 6.2, the header files in the TSAPI Linux SDK are installed with read-only permissions.
- Prior to AE Services 6.2, the TSAPI Windows Client Setup program did not always store the AE Services servers entered during the "AE Services Server Configuration" step in the TSLIB.INI file.
- A buffer overrun in the TSAPI Spy program has been fixed. After a buffer overrun had occurred, any attempt to enable or modify the TSAPI Spy Log to File settings would likely cause the TSAPI Spy program to crash.
- The TSAPI Exerciser now properly sets the level parameter when calling acsOpenStream().
- The TSAPI Exerciser script interpreter now recognizes the no_wait keyword.
- The help file for the TSAPI Exerciser has been updated.

- Within the TSAPI SDKs, the following union members have been removed from the definition of ATTEvent_t in header file attpriv.h:
 - queryAgentMeas
 - querySplitSkillMeas
 - queryTrunkGroupMeas
 - queryVdnMeas
 - queryAgentMeasReq
 - querySplitSkillMeasReq
 - queryTrunkGroupMeasReq
 - queryVdnMeasReq

Support for the services associated with these union members was removed in AE Services 6.1.

• TSAPI Service

- Beginning with AE Services 6.2, the TSAPI Service and private data libraries support private data version 10. Private data version 10 adds private data to the CSTA Logged On event and provides two new private data formatting functions:
 - attV10ConsultationCall() – allows an application to indicate the intended purpose (consult only, conference only, transfer only, or unrestricted) of a cstaConsultationCall() service request.
 - attV10QueryStationStatus() – reports a station’s talk state and service state
- For AE Services 6.2, the default value for the TSAPI Link Advanced Setting “Max Flow Allowed” has been increased from 800 to 2000. This increase will reduce the likelihood of TSAPI applications receiving CSTA Universal Failure Confirmation events with error TSERVER DRIVER CONGESTION. When upgrading to AE Services 6.2 from an earlier release, the new default value will automatically be applied to any existing TSAPI Links using the old default value.
- For AE Services 6.2, the default value for the TSAPI Link Advanced Setting “TSDI Size” has been increased from 2,097,152 to 5,242,880. This increase will reduce the likelihood of TSAPI applications receiving CSTA Universal Failure Confirmation events with errors TSERVER NO TDI BUFFERS and TSERVER NO MEMORY. When upgrading to AE Services 6.2 from an earlier release, the new default value will automatically be applied to any existing TSAPI Links using the old default value.
- For AE Services 6.1.x, the TSAPI Service does not initialize correctly if IPv6 is disabled on the AE Services server. For AE Services 6.2, this has been fixed.

- Prior to AE Services 6.2, in some call scenarios the Single Step Transfer Call service may fail with error RESOURCE BUSY when it should not. In particular, this error may occur if the transfer destination had also been the transfer destination for a prior Single Step Transfer Call service request, and the ASAI Call Alerting event for the transfer destination had arrived after the ASAI Third Party Merge Confirmation event for the transfer request. (This ASAI event sequence has been observed when the transfer destination is a SIP endpoint.) For AE Services 6.2, this problem has been fixed.
- Prior to AE Services 6.2, in some Single Step Transfer Call scenarios the CSTA Delivered event cause and original call information reason may be incorrect. Beginning with AE Services 6.2, the event cause for a CSTA Delivered event resulting from a Single Step Transfer Call service request will be either EC_TRANSFER (for private data versions 2-7) or EC_SINGLE_STEP_TRANSFER (for private data versions 8 and later) instead of EC_NEW_CALL. The original call information reason will be OR_TRANSFERRED instead of OR_NEW_CALL.
- Prior to AE Services 6.2, the Route Register Request service would fail with error OUTSTANDING REQUEST LIMIT EXCEEDED if an application tried to re-register as the routing application for a routing device from a stream opened with the same login ID, application name, and client IP address as the stream used to make the original Route Register Request. Beginning with AE Services 6.2, subsequent Route Register Requests for the same routing device will succeed as long as they are made from a stream opened with the same login ID, application name, and client IP address as the stream used to make the original Route Register Request.
- Beginning with AE Services 6.2 and Avaya Communication Manager 6.2, when an EC500 user makes an outgoing call from his or her mobile phone and then accesses the call from his or her desk set, the event cause in the CSTA Established event will be EC_KEY_CONFERENCE instead of EC_NEW_CALL. (In this scenario, event cause EC_KEY_CONFERENCE has higher precedence than event cause EC_CALL_PARK.)
- Prior to AE Services 6.2, the TSAPI Service did not always provide a CSTA Established event when a bridged party that had dropped off a call later re-joined the same call.
- For AE Services 6.2, TSAPI events for Call Park scenarios have been improved.
- For AE Services 6.2, TSAPI events for Automatic Callback Call scenarios have been improved when the called number is a logical agent ID instead of a station extension.

- Prior to AE Services 6.2, simultaneous Snapshot Call requests for the same call are processed sequentially. Beginning with AE Services 6.2, these requests are processed in parallel.
- Prior to AE Services 6.2, in some call scenarios the Clear Connection service may fail with error OUTSTANDING REQUEST LIMIT EXCEEDED when trying to drop an external party from a conference call.
- Prior to AE Services 6.2, in some transfer scenarios involving the Single Step Conference Call service, the transferred connections list in the CSTA Transferred event may not contain the correct device IDs.
- Prior to AE Services 6.2, in some transfer scenarios involving Service Observing, the transferred device in the CSTA Transferred event may incorrectly contain the extension number of the service observer.
- Prior to AE Services 6.2, the device ID type of the called device in a CSTA Originated event may be incorrect. Beginning with AE Services 6.2, the TSAPI Service uses the address type and numbering plan information from ASAI to set the device ID type of the called device in the CSTA Originated event.
- Prior to AE Services 6.2, in some call scenarios the device ID type of the calling device in a CSTA Route Request Ext event may be incorrect.
- Prior to AE Services 6.2, in some call scenarios the device ID type of the failing device in the CSTA Failed event may be reported as IMPLICIT PUBLIC instead of EXPLICIT PRIVATE LOCAL NUMBER.
- Prior to AE Services 6.2, in some call scenarios the device ID type of a dynamic device ID may be reported as IMPLICIT PRIVATE instead of EXPLICIT PUBLIC UNKNOWN.
- Prior to AE Services 6.2, the last redirection device in the CSTA Queued event may be incorrect when a call is queued to one or more skills and a converse-on vector step directs the call to another skill.
- Prior to AE Services 6.2, in some Make Predictive Call scenarios the device ID types in the associated CSTA unsolicited events are incorrect.
- Prior to AE Services 6.2, in some Make Predictive Call scenarios the results of the Snapshot Call service did not include the called party from the Make Predictive Call service request.

- Prior to AE Services 6.2, if Universal Call IDs (UCIDs) are not enabled on Avaya Communication Manager, then for private data versions 5 and later, private data will incorrectly accompany the CSTA Service Initiated event resulting from an ASAI Third Party Auto Dial request (e.g., a Make Call service request). Beginning with AE Services 6.2, private data will not accompany the CSTA Service Initiated event in this case.
- Prior to AE Services 6.2, for private data versions 7 and later, private data does not accompany a CSTA Route Request Ext event when the only private data to report is the ISDN redirecting number. Beginning with AE Services 6.2, private data will accompany the CSTA Route Request Ext event in this case.
- Prior to AE Services 6.2, the TSAPI Service could crash when sending an ACS Client Heartbeat event to a client application using a secure Tlink.
- A buffer overrun in the TSAPI Service message tracing facility has been fixed. When a buffer overrun occurred, the TSAPI Service could crash.
- Beginning with AE Services 6.2, Device IDs with Device Type “TRUNK GROUP” may be administered in the Security Database. (The Monitor Device service is the only TSAPI service that recognizes trunk group device IDs; an ISDN PRI trunk group may be monitored to receive ATT Charge Advice events when the Avaya CM Advice of Charge feature is active.)
- Prior to AE Services 6.2, the TSAPI Service sometimes represented integer values in error messages using hexadecimal instead of decimal. Beginning with AE Services 6.2, most integer values in error messages appear in decimal. When values appear in hexadecimal, they are explicitly prefixed with “0x”.