



Avaya Aura[®] Application Enablement Services

R6.1 Server and Client Release Notes

Issue 1.2

August 2011

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Release 6.1 and describes important notes and known issues.

WHAT'S CHANGED IN AE SERVICES 6.1?

- Processor Ethernet connections can be utilized in Enterprise Survivable Server (ESS) and Local Survivable Processor (LSP) environments. Customers can choose which ESS and LSP node to use while running in a fragmented state.
- .NET DMCC clients support the following operating systems:
 - Windows 7 Professional (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Enterprise (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Ultimate (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows Server 2008 R2 (64-bit in 32-bit compatibility mode)
 - Windows XP Professional (32-bit)
 - Windows 2003 Server Standard Edition (32-bit)
- A unified API for DMCC call control services (including Java, XML and SDKs) with a key focus on enabling Microsoft.NET developers to adopt AES for CTI-based applications.
- TSAPI clients support the following operation systems:
 - RHEL 5 (32-bit and 64-bit in 32-bit compatibility mode)
 - RHEL 4 (32-bit)
 - Windows 7 Professional (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Enterprise (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Ultimate (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows Server 2008 R2 (64-bit in 32-bit compatibility mode)
 - Windows XP Professional (32-bit)
 - Windows 2003 Server Standard Edition (32-bit)

- CVLAN clients support the following operation systems:
 - RHEL 5 (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Professional (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Enterprise (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows 7 Ultimate (32-bit and 64-bit in 32-bit compatibility mode)
 - Windows Server 2008 R2 (64-bit in 32-bit compatibility mode)
 - Windows XP Professional (32-bit)
 - Windows 2003 Server Standard Edition (32-bit)
- AE Services Sametime integration can operate in the following configurations:
 - Sametime community cluster with multiplexer co-resident on the Sametime server
 - Sametime community cluster with multiplexer on separate servers
 - Multiple Sametime community clusters with multiplexers on separate servers
 - Load balancer in front of Sametime community cluster
- IPv6 addressing for connections to Communication Manager 6.0 or later is supported.
- IPv6 addressing for the AE Services server and clients are supported.
- The Historical Metric Data Collector which enables collection, storage and viewing of AE Services metrics.
- Third-party call control of remote station associated with a SIP endpoint.
- ASAI, DMCC, TSAPI and associated API and client enhancements to support Avaya Aura® Contact Center (AACC).
- A new parameter called “Networking | TCP Settings | TCP Retransmission Count” was added to the AE Services Management Console. The allowed TCP Retransmission Count range is from 2 through the default value of 15. A smaller TCP Retransmission Count reduces the amount of time that the AE Services server waits for a TCP acknowledgement from an unresponsive client application before closing the socket
- SIP stack changes:
 A new parameter called “cmapl.nist_max_server_transactions” was added to the /opt/mvap/user-configuration.properties. The recommended setting for this parameter is 1.25 times the number of SIP users expected to use the AE Services server with a default value of 5,000. The SIP stack uses this parameter to establish a low threshold for dropping messages under heavy traffic conditions.

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 6.1 CVLAN Client Linux 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-linux-6.1-396.i386.rpm
Avaya Aura® Application Enablement Services 6.1 CVLAN Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	cvlan-client-win32-6.1-396.zip
Avaya Aura® Application Enablement Services 6.1 TSAPI Client Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-linux-6.1-396.i386.rpm
Avaya Aura® Application Enablement Services 6.1 TSAPI Client MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-client-win32-6.1-396.zip
Avaya Aura® Application Enablement Services 6.1 TSAPI SDK Linux 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-linux-6.1-396.i386.rpm
Avaya Aura® Application Enablement Services 6.1 TSAPI SDK MS Windows 32-bit and 64-bit in 32-bit compatibility mode	tsapi-sdk-win32-6.1-396.zip
Avaya Aura® Application Enablement Services 6.1 JTAPI SDK	jtapi-sdk-6.1.0.77.zip
Avaya Aura® Application Enablement Services 6.1 Web Service - System Management SDK	smssvc-sdk-6.1.0.501.zip
Avaya Aura® Application Enablement Services 6.1 DMCC .Net SDK 32-bit and 64-bit in 32-bit compatibility mode	dmcc-dotnet-sdk-6.1.0.37.zip
Avaya Aura® Application Enablement Services 6.1 Web Services - Telephony SDK 32-bit and 64-bit in 32-bit compatibility mode	telsvc-sdk-6.1.0.501.zip
Avaya Aura® Application Enablement Services 6.1 DMCC XML SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapixml-sdk-6.1.0.497.zip
Avaya Aura® Application Enablement Services 6.1 DMCC Java SDK 32-bit and 64-bit in 32-bit compatibility mode	cmapijava-sdk-6.1.0.497.zip
Avaya Aura® Application Enablement Services 6.1 Software Only 32-bit and 64-bit in 32-bit compatibility mode	swonly-r6-1-0-20-20110106.iso
Avaya Aura® Application Enablement Services 6.1 Hardware Bundled Upgrade for S8510 32-bit and 64-bit in 32-bit compatibility mode	bundled-r6-1-0-20-20110106.iso
Avaya Aura® Application Enablement Services 6.1 on System Platform 32-bit and 64-bit in 32-bit compatibility mode	aes-r6-1-0-20.iso
System Platform Service Pack R6.0.2	vsp-6.0.2.0.5.iso
System Platform Patch R6.0.2.3.5	vsp-patch-6.0.2.3.5.noarch.rpm
Avaya Aura® Application Enablement Services Product MIBs	aesvcs-product-mibs-6.1.0.501.zip
Standard MIBs	standard-mibs-6.1.0.501.zip

IMPORTANT NOTES

- AE Services 6.1 supports Red Hat Enterprise Linux 5.0 Update 5.
- AE Services 6.1 is compatible with the following Bundled Server: Dell 1950 (S8510)
- AE Services 6.1 on System Platform is compatible with the following Servers:
 - IBM x3550 M2 (S8800)
 - Dell R610
- AE Services 6.1 on System Platform is compatible with the following versions of System Platform:
 - System Platform R6.0.2
- AE Services 6.1 is compatible with the following Communication Manager Releases and Platforms:
 - Communication Manager 4.x (S8300, S8400, S8500, S87xx) - with the following limitation: Once Communication Manager 4.x reaches its End of Manufacturers Support, AE Services 6.1 support of Communication Manager 4.x is limited to any issues that can solely be addressed in the AE Services software.
 - Communication Manager 5.0 (S8300, S8400, S8500, S87xx)
 - Communication Manager 5.1 (S8300, S8400, S85xx, S87xx)
 - Communication Manager 5.2 (S8300, S8400, S85xx, S87xx)
 - Communication Manager 5.2.1 (S8300, S8400, S85xx, S87xx, S8800)
 - Communication Manager 6.0 (S8300D, S8510, S8800)
 - Communication Manager 6.0.1 (S8300D, S8510, S8800)
- Communication Manager 6.0.1 is compatible with the following AE Services Releases:
 - AE Services 4.2.2 Super Patch 4 or later
 - AE Services 5.2.x
- MAPD is NOT supported beginning with Communication Manager 5.0

Avaya SIP Endpoints Supported by AE Services TSAPI

Endpoint	Administ ered as	Endpoint Firmware	AE Services Release	CM/ASM Pair		General Telephony	Agent Features
				CM- ES Version	ASM Version		
9620	9620SIP	2.6 SP5	6.1.x	6.O.1	6.O SP2	yes	no
9640	9640SIP	2.6 SP5	6.1.x	6.O.1	6.O SP2	yes	no
9640G	9640SIP	2.6 SP5	6.1.x	6.O.1	6.O SP2	yes	no
9630G	9600SIP	2.6 SP5	6.1.x	6.O.1	6.O SP2	yes	no
9650	9600SIP	2.6 SP5	6.1.x	6.O.1	6.O SP2	yes	no
9608	9640SIP	6.1	6.1.x	6.O.1	6.O SP2	yes	no
9611	9640SIP	6.1	6.1.x	6.O.1	6.O SP2	yes	no
9621	9640SIP	6.1	6.1.x	6.O.1	6.O SP2	yes	no
9641	9640SIP	6.1	6.1.x	6.O.1	6.O SP2	yes	no

Endpoint	Administ ered as	Endpoint Firmware	AE Services Release	CM/SES Pair		General Telephony	Agent Features
				CM Version	SES Version		
9620	9620SIP	2.5(GA)	5.2.x	5.2.1	5.2.1	yes	no
9640	9640SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9640G	9640SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9630G	9600SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
9650	9600SIP	2.6	5.2.x	5.2.1	5.2.1	yes	no
16CC	4620SIPC C	SIP16CC_1_0_1 2_010_b001.bin	5.2.x	5.2.1	5.2.1	yes	yes (note 1)

Note 1 - Agent Buttons Supported:

Agent login/logout
 After call work
 Auxiliary work
 Auto/manual in
 Release
 Agent Event Package (16CC)

Release History:

Date	Server Build	Change(s)
03/2007	47-3	General Availability R4.0
06/2007	50-1	General Availability R4.0.1
12/2007	31-2	General Availability R4.1
04/2008	4.1.16	General Availability R4.1.1 JTAPI Client/SDK
05/2008	19-4	General Availability R4.2
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	General Availability R5.2
02/2010	103	Service Pack R5.2.1
06/2010	105	Service Pack R5.2.2
02/2011	20	General Availability R6.1

KNOWN ISSUES AND WORKAROUNDS

- **AE Services Manual Database restore from 3.x release requires OAM re-login**

When manually restoring a 3.x database from the AE Services Management Console, be sure to log-out after the restore and then log back in before performing any administration. This is required to synchronize user passwords and if not performed, certain administrative functions such as User Management may not be available from OAM until the re-login.

- **ASAI – The collect digits option in the route select message is no longer supported**

There is a feature that is documented in the ASAI Technical reference (no longer published) where an application can ask in a Route Select message to collect digits.

Implications for TSAPI include: When sending private data with a `cstaRouteSelectInv()` service request, the `collectCode` parameter passed to `attV7RouteSelect()`, `attV6RouteSelect()`, or `attRouteSelect()` should be initialized with a Collect Code Type of `UC_NONE`.

Implication JTAPI include: Method `LucentRouteSession.selectRouteAndCollect()` is not supported. If invoked, it will throw a `TsapiMethodNotSupportedException`.

- **CVLAN Linux Client**

Before installing the CVLAN Linux client on a Red Hat Linux ES v5.0 system, you may need to perform a separate installation of the following RPM:

`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>.

- **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.

- **CVLAN and DLG Services may not show the correct license mode after recovering from restricted mode with the AE Services on System Platform Offer with High Availability**

If the CVLAN service enters license restricted mode and the licensing error is fixed, the license mode may still appear to be restricted even though the CVLAN service is functioning normally. This will occur if any of the administered CVLANs do not have the "proprietary" check box selected.

If the DLG service enters license restricted mode and the licensing error is fixed, the license mode will still appear to be restricted even though the DLG service is functioning normally.

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

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. 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. Suppressing bridged call appearances for the station 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.

- **Email notifications will not be issued after installing or upgrading to AE Services 6.1**

This will affect all customers who used the "Email Notification" feature in AE Services 5.2 and higher.

When Email Notification is Enabled from AE Services Management Console using the "Utilities | Email Notification" screen, be sure to do the following steps:

- 1) Login to the AE Server as a user with root privileges and execute the remaining steps from the command line.

```
2) /bin/sed -i 's/CATALINA_HOME/common/CATALINA_HOME/'  
/opt/mvap/bin/sentemail.sh  
3) /bin/sed -i 's/406/407/' /opt/mvap/bin/sentemail.sh  
4) /bin/sed -i 's/CATALINA_HOME/common/CATALINA_HOME/'  
/opt/mvap/watchdog/bin/watchdogEmail
```

- **Firewall changes requiring restart are service affecting**

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

When attempting to connect to the AE Server's IPv6 address using the DMCC Java SDK from Microsoft Windows, the user will see the following error message: "java.net.SocketException: Address Family not supported by protocol family"

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

- **Local WebLM Server Port Number**

If you have upgraded to AE Services 6.1 from an earlier release of AE Services, your 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 your 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".
5. For the Bundled or AE Services on System Platform Server offers, select "Security | Standard Reserved Ports".
6. If the "TOMCAT HTTPS – 8443" row is not checked, then click it and click "Apply".

After changing the WebLM Port to 443, you must 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".

- **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. Sign-out of OC and then sign-in again to re-establish phone integration.

- **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 Auth. 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 box for the TSAPI, Transport, asailink, DLG or CVLAN services, 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 date/time 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 box for the TSAPI, Transport, asailink, DLG or CVLAN services, and then click on "Start".

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

<http://support.avaya.com/css/P8/documents/100068114>

- **TSAPI Linux Client**

Before installing the TSAPI Linux client on a Red Hat Linux ES v5.0 system, you may need to perform a separate installation of the following RPM:

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>.

- **TSAPI Windows Client “Edit TSLIB.INI” Shortcut Issue**

When Release 6.1 of the TSAPI Windows Client is installed on a 64-bit Windows system where an older version of the TSAPI Windows Client had been installed previously, Windows may report an error (for example, "Shortcut Missing") when you select the "Avaya AE Services | TSAPI Client | Edit TSLIB.INI" shortcut from the Start menu.

To address this issue, locate the TSLIB.INI file from the previous installation (the default location is "C:\Program Files\Avaya\AE Services\TSAPI Client\TSLIB.INI"), and copy it to the target location for the shortcut (by default, "C:\Program Files (x86)\Avaya\AE Services\TSAPI Client\TSLIB.INI").

To determine the target location for the shortcut:

1. Select "Avaya AE Services | TSAPI Client" from the Start menu
2. Right-click on the "Edit TSLIB.INI" shortcut and select "Properties".

3. When the "Edit TSLIB.INI Properties" dialog box appears, select the "Shortcut" tab. The "Target" field provides the target location for the shortcut.
4. Click "Cancel" to close the "Edit TSLIB.INI Properties" dialog box.

- **Reserving TSAPI User Licenses**

After installing or upgrading to AE Services 6.1, Avaya recommends that you follow this procedure to ensure that the TSAPI Service starts successfully after a system reboot and to optimize the performance of the TSAPI Service:

1. Determine your WebLM configuration model.

In a typical AE Services configuration, a standard license file is installed on each AE Services server, and the licenses in that license file are acquired through a local WebLM server running on the AE Services server or CDOM for the AE Services on System Platform Server. However, other configurations are also possible:

Multiple AE Services servers may be configured to acquire their feature licenses from a single WebLM server where a standard license file is installed. In this configuration, feature licenses can "float" from one AE Services server to another as they are needed.

With Enterprise Wide Licensing, an enterprise license file is installed on a master WebLM server. Feature licenses can be allocated from the enterprise license file to multiple AE Services servers, where they are acquired by the local WebLM server. If any of the feature licenses from the enterprise license file are not allocated to the individual AE Services servers, then these feature licenses can also float among the AE Services server.

For AE Services 5.2, the use of floating licenses is **not** recommended. Adjust your WebLM configuration as appropriate if you are using floating licenses.

2. Log into the Application Enablement Services Management Console and select "Licensing | WebLM Server Access" to access the WebLM Logon screen. (The WebLM Logon screen should be displayed in a new browser window.)
3. Log into WebLM and select "Application_Enablement" to display the AE Services licensed features.
4. Note the number of TSAPI Simultaneous Users (VALUE_TSAPI_USERS) that are licensed.
5. From the AE Services Management Console, select "Licensing | Reserved Licenses". The Reserved Licenses page is displayed.

6. In the "Reserved TSAPI Basic User Licenses" field, enter the value that you recorded in Step 4 above, and then click "Apply Changes". When asked to confirm the change, click "Apply".
7. From the AE Services Management Console and select "Maintenance | Service Controller".
8. Set the check box for "TSAPI Service" and click on the "Restart Service" button. When the confirmation screen is displayed, click on the "Restart" button.

- **Sametime Upgrade from 8.0 to 8.02 Loses the Telephony Service Provider Policy Setting**

When Sametime is upgraded from 8.0.0 to 8.0.2, the telephony service provider is not enabled as a default. Re-enable the Telephony Service Provider field in the Sametime Policy.

The IBM SPR is SLEE7NKJRJ.

- **Sametime Connect 8.0.2 – Calls Cannot Be Made to the Client when “Display Incoming Invitation” Is Unchecked**

When a Sametime client unchecks "Preferences | Notifications | Telephony notifications | Display incoming invitation" in Sametime Connect 8.0.2, Sametime calls cannot be made to that particular client. IBM has provided Hotfix # DAMD-7NJKJA.

- **SNMP**

The SNMP GET related to the amount of memory associated with the DMCC Service (avAesDmccUsedMemory.0, avAesDmccFreeMemory.0, and avAesDmccMaxMemory.0) is incorrectly calculated.

- **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 direct agent call to a busy agent on a SIP endpoint, the call drops. The workaround is to place the call manually.
- When using 3rd party call control to make a call using a TAC, the call will fail on a SIP phone if the Communication Manager does not have a TN2602AP board.
- When using 3rd party call control to answer and place a call on hold on a SIP endpoint any attempt to make another call from that SIP endpoint will fail.

- 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 service does not work reliably for SIP stations.
- User classified call does not generate an ALERTING event over an ASAI domain control association.
- Going off-hook on a SIP station followed by on-hook does not generate an INITIATED event.
- Using Third 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.

• **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

• **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.

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 R6.0.2 release notes at

<https://support.avaya.com/css/Products/P0585/Release%20Notes%20&%20Software%20Update%20Notes>

SYSTEM PLATFORM SERVICE PACK PATCH 6.0.2.3.5

The patch addresses the following issues:

1. WebLM certificate expiration on March 31st, 2011.
2. Dell R610 and HP DL 360 server sensor issues.
3. Windows HVM copy issues.

RESOLVED ISSUES IN AE SERVICES RELEASE 6.1

• AE Services Server

- During the upgrade process, an operation, which required the AE Services internal database to be in a running state, was attempted against the database, while in a stopped state. This action had the potential to cause the upgrade process to hang. Before the upgrade process starts, the database is stopped. Once the attempted operation is invoked, it would make several attempts to acquire a connection to the database. This operation was modified to occur after the upgrade process completes in order to allow the database to be fully operational.
- A race condition existed during the upgrade process which had the potential to prevent the upgrade process from automatically restoring the server data during the post upgrade stage.
- For a non-root user, the incorrect status was returned for the database service when queried by a system administrator. The database status command was modified to return the correct status for non-root system admin users.
- The CPU occupancy was not checked for high usage during the first 20 minutes for the start of each day (from 12:00 AM to 12:20 AM) because of a calculation error. The specified error has been resolved.
- After an install, upgrade, or server data restore process, the root account was incorrectly modified to expire after 60 days.
- The PostgreSQL database stopped accepting requests because of a potential transaction ID wrap around on the default database called “postgres”. The cron script used to periodically execute a vacuum of the AE Services database was updated to include the postgres default database. The vacuum process is beneficial in the prevention of transaction ID wrap around. In addition, the database log file configuration parameters were updated to properly cause the database log files to roll-over weekly. Previously, a new log file was created daily and the old logs were not removed.
- Tomcat rollover capability is now configurable. The default rotate number is 5 and the size is 1M. Edit the “/etc/logrotate.d/catalinaoutrate” file to reconfigure the rotate parameter.
- Previously, after a restore on an AE Services server, Tomcat was not restarted if a certificate existed. The restart of Tomcat and httpd has been automated after a restore. In addition, the restart of Tomcat and https confirmation was added to OA&M, during a data restore from OA&M (if a certificate exists).

- Previously, OA&M did not check if an uploaded file completely loaded resulting in corruption issues. In AE Services 6.1, OA&M will verify if the upload completed. If the file did not completely load, the error message "Upload failed: unexpected end of file" will be displayed and the restore will stop.
- The md5 checksum is now displayed on the "Backup" page to compare the checksum of a downloaded file.
- Updated Tomcat version from 5.5.26 to 6.0.29 (latest version) - <http://tomcat.apache.org/tomcat-6.0-doc/changelog.html>

• **CVLAN Clients and SDKs**

- The setup program for the CVLAN Windows client and SDK has been rewritten for AE Services 6.1.

Note to developers of CVLAN Windows applications: The old setup program installed the file cvlancli.lib in the Windows system32 folder. The new setup program installs this file in the lib subfolder of the installation folder.

- Beginning with AE Services 6.1, the CVLAN clients support IPv6.

• **CVLAN Server**

Beginning with AE Services 6.1, the CVLAN Server supports IPv6 client connections.

• **DLG Server**

Beginning with AE Services 6.1, the DLG Server supports IPv6 client connections.

• **DMCC**

- To support the 3.x SDK with AE Services 6.1, the property "cmapi.is3dotxsdk" on "/opt/mvap/conf/user-configuration.properties" was added. If the SDK is version 3.x, set the "cmapi.is3dotxsdk" to true; otherwise, set the "cmapi.is3dotxsdk" to false. If using version 4.x or 5.x SDKs mixed with 3.x SDKs, upgrade the 3.x versions.
- System Platform LDAP users can now run the java-jdk tutorial and the TSAPI test from the AE Services OAM console.
- Previous, the DMCC secure socket failed to come up if a server certificate request (CSR) had been created but had not been administered. In AE Services 6.1, if there isn't a server certificate, the DMCC secure socket will use the default certificate.

- **JTAPI**

Updated the Java SDK license file and incorporated a list of redistributable files in the SDK license file.

- **Licensing**

- Prior to AE Services 6.1, when WebLM displayed the licenses acquired by the TSAPI, CVLAN, and DLG services, it provided the fully qualified domain name of the AE Services server. Beginning with AE Services 6.1, WebLM only provides the host name of the AE Services server.
- Added a new "Reserved Licenses" link under the "Licensing" tab, which can be used to configure the number of "Reserved TSAPI Basic User Licenses", "Reserved Unified Desktop Licensed" and "Reserved DMCC License".
- Enterprise Web Licensing is supported on AE Services on System Platform 6.1.

- **.NET**

- Provided clarity for customers using the .NET dashboard tool for the features which require a "Session ID" by highlighting the "Session ID" label on the dashboard when the user hovers the mouse over the "Reconnect", "Get Device ID List", "Get Monitor List" or the "Transfer Monitor Object" button.
- Agent information ("agentName", "agentLoginID" and "agentStationExtension") available in a "GetCallInformation" response after a "DeliveredEvent" is received was not included in the "GetCallInformation" response after the "EstablishedEvent" is received for the same call. The agent information now remains available in a "GetCallInformation" for the call after the "EstablishedEvent" is received.
- Updated the .NET SDK license file and incorporated a list of redistributable files in the SDK license file.
- The .NET SDK was not including the Alert time value in the "MakePredictiveCall" request even though a valid value was specified by the application developer.
- The .NET SDK log file was not configured properly to roll over, allowing the log file to grow exponentially.
- Using the .NET dashboard tool, duplicate device instances were shown in the "Device ID" listbox after a "Transfer Monitor Object" response was received if both the transferor and transferee session object contained a reference to the same "Device ID" instance.

- Using the .NET SDK, the “EstablishedEventArgs” class did not expose the UCID or “localConnection” data even though the UCID and “localConnection” attribute were included in the XML response from AE Services when a call was established.
- Using the .NET SDK ActiveX Controller, the “GetCallInformationResponseEvent” was not triggered when a “GetCallInformation” response was received by the client.
- The .NET dashboard tool kept a reference to a “Device ID” instance after it was successfully released using the “Release Device ID” request. As a result, a second “Release Device ID” request was issued for a device once the session is stopped using the dashboard.
- Added support in the “Single Step Transfer Call” response for the “SingleStepTransferCallResponsePrivateData” item UCID. In addition, access was provided to the “called” and “transferee device ID” via the “SingleStepTransferCallResponseArgs” class.
- The .NET SDK and the dashboard tool includes support for the “Reconnect Call” optional private data items “Drop Resource” and “User Data” in AE Services 6.1.
- The .NET SDK ActiveX Controller includes support for the “Reconnect Call” optional private data items “Drop Resource” and “User Data” in AE Services 6.1.
- Provided support in the .NET SDK and dashboard tool for the “User Data” field missing from the “Consultation Call” request.
- In the dashboard tool, under the "Automated Testing" tab, a monitor start request based on the dashboard's “Start Monitor” button was not saved properly to the script file in order to mimic the real individual button objects for each monitor. Therefore, when the saved script was executed, the monitor start request step was not properly executed.
- “GetMonitorList” results were not configured correctly in the “GetMonitorListEventArgs” response by the .NET SDK. The data related to a Session Management Monitor is not populated in the “GetMonitorListEventArgs” object and the remaining SDK monitors include results that did not pertain to them. In addition, the results were not displayed correctly in the dashboard.
- The session duration timer is used to calculate when to send a “ResetApplication” heartbeat to the AE Services server. The proper range of the session duration timer is from 30 seconds to 7,200 seconds (2 hours). When the request is sent to the AE Services server, it validates the request

and sends the negotiated value in the response. In previous releases, the .NET SDK did not use the time period returned in the “ResetApplication” response. Instead the .NET SDK would incorrectly accept any session duration time provided by an application developer.

- Provided a method in the “CallInformationEventArgs” class to obtain the “agentName” from the “CallInformationResponseEvent” via the .NET SDK and ActiveX Controller.
- Using the .NET SDK for a “Transfer Monitor Object” request, the data related to a transferred “Session Management Monitor”, “Call Information” monitor, and “Private Only” data for the monitors Phone, Media, and Call Control was not populated in the “TransferMonitorObjectsEventArgs” object. The dashboard tool was not displaying the transferred monitors in the “Monitor ID” textbox. In the “Events” section of the dashboard which is used to display the data of the “TransferMonitorObjectsEventArgs” object, the monitor data display included results that do not pertain to them. This issue has been resolved in R6.1.
- The dashboard tool incorrectly highlighted the “Device ID” listbox text when the mouse is hovered over the “Start Call Information Monitor” button.
- Using the dashboard tool, the “Consultation Call” request did not populate the “Private Data” item type of call for a supervisor-assist call in the issued request.
- For a “Release Device ID” request using the dashboard tool, the dashboard was incorrectly removing all the monitors from the dashboard’s “Monitor ID” listbox based on the monitors associated “Session ID” instead of the monitor “Device ID”. As a result, if a session had more than one device with associated monitors, all the monitors related to the “Session ID” will be removed from the dashboard’s “Monitor ID” listbox.
- In the .NET SDK, the “Clear Connection” request did not include support for “User Data”. The SDK was modified to include a new inner class called “ThirdPartyCallController.ClearConnectionParameters” and a new overloaded method called “ThirdPartyCallController.ClearConnection” which takes the new parameter class object as one of its params. The new parameters object contains the “CallConnectionID”, “PrivateData” and “UserData”.
- In order to alleviate congestion on the .NET SDK TCP receive buffer which would result in the possible closure of the .NET session socket when under a heavy load, a new property was introduced to allow an application developer the ability to adjust the TCP receive buffer size.

- Added support in the .NET SDK to report session termination reason to a client application.

• Security

- The following Red Hat Linux security issues have been incorporated into Release 6.1:
 1. [RHSA-2009:1452] Moderate: neon security update
 2. [RHSA-2009:1471] Important: elinks security update
 3. [RHSA-2009:1463] Moderate: newt security update
 4. [RHSA-2009:1484] Moderate: postgresql security update
 5. [RHSA-2009:1548] Important: kernel security and bug fix update
 6. [RHSA-2009:1625] Moderate: expat security update
 7. [RHSA-2009:1646] Moderate: libtool security update
 8. [RHSA-2009:1648] Moderate: ntp security update
 9. [RHSA-2009:1670] Important: kernel security and bug fix update
 10. [RHSA-2010:0046] Important: kernel security and bug fix update
 11. [RHSA-2010:0122] Important: sudo security update
 12. [RHSA-2010:0144] Moderate: cpio security update
 13. [RHSA-2010:0141] Moderate: tar security update
 14. [RHSA-2010:0149] Important: kernel security and bug fix update
 15. [RHSA-2010:0162] Important: openssl security update
 16. [RHSA-2010:0163] Moderate: openssl security update
 17. [RHSA-2010:0165] Moderate: nss security update
 18. [RHSA-2010:0168] Moderate: httpd security and enhancement update
 19. [RHSA-2010:0178] Important: Red Hat Enterprise Linux 5.5 kernel security and bug fix update
 20. [RHSA-2010:0198] Moderate: openldap security and bug fix update
 21. [RHSA-2010:0258] Low: pam_krb5 security and bug fix update
 22. [RHSA-2010:0273] Moderate: curl security, bug fix and enhancement update
 23. [RHSA-2010:0329] Moderate: curl security update
 24. [RHSA-2010:0343] Important: krb5 security and bug fix update
 25. [RHSA-2010:0360] Moderate: wireshark security update
 26. [RHSA-2010:0361] Moderate: sudo security update
 27. [RHSA-2010:0398] Important: kernel security and bug fix update
 28. [RHSA-2010:0423] Important: krb5 security update
 29. [RHSA-2010:0429] Moderate: postgresql security update
 30. [RHSA-2010:0457] Moderate: perl security update
 31. [RHSA-2010:0458] Moderate: perl security update
 32. [RHSA-2010:0475] Moderate: sudo security update
 33. [RHSA-2010:0504] Important: kernel security and bug fix update
 34. [RHSA-2010:0542] Moderate: openldap security update
 35. [RHSA-2010:0543] Moderate: openldap security update
 36. [RHSA-2010:0578] Important: freetype security update
 37. [RHSA-2010:0607] Important: freetype security update
 38. [RHSA-2010:0610] Important: kernel security and bug fix update

- 39. [RHSA-2010:0616] Moderate: dbus-glib security update
 - 40. [RHSA-2010:0625] Moderate: wireshark security update
 - 41. [RHSA-2010:0659] Moderate: httpd security and bug fix update
 - 42. [RHSA-2010:0660] Important: kernel security and bug fix update
 - 43. [RHSA-2010:0661] Important: kernel security update
 - 44. [RHSA-2010:0675] Important: sudo security update
 - 45. [RHSA-2010:0676] Important: kernel security update
 - 46. [RHSA-2010:0677] Important: kernel security update
 - 47. [RHSA-2010:0678] Moderate: rpm security update
 - 48. [RHSA-2010:0679] Moderate: rpm security and bug fix update
 - 49. [RHSA-2010:0681] Critical: firefox security update
 - 50. [RHSA-2010:0703] Important: bzip2 security update
 - 51. [RHSA-2010:0723] Important: kernel security and bug fix update
 - 52. [RHSA-2010:0737] Important: freetype security update
 - 53. [RHSA-2010:0779] Moderate: kernel security and bug fix update
 - 54. [RHSA-2010:0787] Important: glibc security update
 - 55. [RHSA-2010:0792] Important: kernel security update
 - 56. [RHSA-2010:0793] Important: glibc security update
 - 57. [RHSA-2010:0819] Moderate: pam security update
 - 58. [RHSA-2010:0839] Moderate: kernel security and bug fix update
- Updated php version from 5.2.9 to 5.2.14 (latest 5.x version) - <http://www.php.net/ChangeLog-5.php#5.2.14>
 - Incorporated RHEL TCP Denial of Service fixes: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609> , <https://access.redhat.com/kb/docs/DOC-18730>
 - Incorporated general security hardening according to security best practices for:
 - Apache web server
 - PostgreSQL database server
 - OpenLDAP server
 - Added the new link "Default Certificates" under "Security" | "Certificate Management" | "Server Certificates" to display AE Services default certificates.
- **SNMP**
 - A daily SNMP Trap and alarm will be generated after the AE Services license or AE Services certificate expires.
 - During an upgrade from AE Services release 4.0, on the AE Services Bundled server, an upgrade not committed alarm and SNMP Trap is generated after a server reboot.

- All unacknowledged alarms will be removed after 30 days to prevent a possible negative affect on the performance of the database.
- **TSAPI Client Libraries and SDKs**
 - The TSAPI Windows client setup program and SDK setup program have been rewritten for AE Services 6.1. Searches of the user's hard drive have been eliminated, reducing the installation time.
 - Beginning with AE Services 6.1, the TSAPI clients support IPv6.
 - The TSAPI private data libraries have been updated to provide support for private data version 9. Private data version 9 introduces:
 - A new version of the ATT Single Step Transfer Confirmation Event that provides the Universal Call ID (UCID) of the resulting call.
 - The notion of a consultation mode for the CSTA Held, Service Initiated, and Originated events. The consultation mode allows applications to determine whether those events were the result of a Conference button press at the telephone set, a Transfer button press at the telephone set, or an invocation of the Consultation Call service.
 - Prior to AE Services 6.1, the default size of the send and receive queues for the TSAPI Windows client was 2. Beginning with AE Services 6.1, the default size of the send queue is 4 and the default size of the receive queue is 16.
 - Prior to AE Services 5.2.1, the TSAPI Spy program could display a sharing violation error when enabling the "Log to File" option. This issue has been resolved.
 - Prior to AE Services 4.2.4 and in AE Services 5.2.x, the TSAPI Windows client library could cause an application to crash if a stream opened by the application had failed. This issue has been resolved.
 - Prior to AE Services 6.1, the TSAPI Windows client library could cause an application to crash if an application thread is sending or receiving data on a stream while another thread is in the midst of closing or aborting the stream.
 - Prior to AE Services 4.2.4, AE Services 5.2.2, and AE Services 6.1, when using an encrypted Tlink, an intermittent error condition could cause the TSAPI Windows client library to close a stream with ACS error TSERVER STREAM FAILED.
 - Support for simulator sessions and simulator administration has been removed from the TSAPI Exerciser, a component of the TSAPI Windows SDK. (The Avaya MultiVantage Simulator was included with the Avaya Computer Telephony offering, but is not included with AE Services.)

- The makefiles for the sample applications provided with the TSAPI Windows SDK have been updated. Prior to AE Services 6.1, the sample applications did not compile successfully when using the provided makefiles.
- Prior to AE Services 5.2.2, installation of the TSAPI Linux client required OpenSSL version 0.9.8 or later. For AE Services 6.1, installation of the TSAPI Linux client only requires OpenSSL version 0.9.7 or later.
- Prior to AE Services 6.1, the TSAPI Service might close a connection to an idle TSAPI Linux client that did not poll for events at regular intervals. Beginning with AE Services 6.1, the TSAPI Linux client library will consume heartbeat messages from the TSAPI Service so that its TCP receive queue does not fill up.
- Prior to AE Services 6.1, the tracing mechanism for the TSAPI Linux client would output invoke IDs and cross reference IDs in hexadecimal notation. Beginning with AE Services 6.1, these values are output in decimal notation.
- The following header files in the TSAPI SDKs have been replaced by the new header file ossship.h:
 - asn1code.h
 - asn1glob.h
 - asnihdr.h
 - ossdll.h
 - ossglob.h

The following header files have been removed from the TSAPI SDKs because they are no longer relevant for the AE Services product:

- cticoamdefs.h
- cticvrdefs.h
- ctisdbdefs.h
- ctitoamdefs.h
- drvrrdefs.h
- sdb.h
- sdbdefs.h
- tdrvrr.h

- **TSAPI Service:**

- Beginning with AE Services 6.1, the TSAPI Service supports IPv6 client connections.
- The TSAPI Service has been updated to provide support for private data version 9. Private data version 9 introduces:

- A new version of the ATT Single Step Transfer Confirmation Event that provides the Universal Call ID (UCID) of the resulting call.
- The notion of a consultation mode for the CSTA events Held, Service Initiated, and Originated. The consultation mode allows applications to determine whether those events were the result of a Conference button press at the telephone set, a Transfer button press at the telephone set, or an invocation of the Consultation Call service.
- The Alternate Tlinks feature has been enhanced to handle scenarios where the CTI link between AE Services and Avaya Communication Manager (CM) is down.
 - Prior to AE Services 6.1, the Alternate Tlinks feature could be used to direct the TSAPI client library to select a different Tlink when opening a stream if the client library could not locate the preferred Tlink. The feature supported scenarios where the client was unable to communicate with the AE Services server or where the TSAPI Service was not online, but did not support scenarios where the CTI link between the AE Services server and CM was down.
 - Beginning with AE Services 6.1, the TSAPI Service can be configured not to advertise Tlinks when the CTI link between the AE Services server and the CM associated with that Tlink is down. When the TSAPI Service is configured in this way, the Alternate Tlinks feature will try to select an alternate Tlink if the preferred Tlink is not in service.
- Beginning with AE Services 6.1, TSAPI security database policies have changed. A TSAPI user must have Call Origination/Termination and Device Status permissions in the Security Database in order to use the following TSAPI services:
 - cstaQueryMsgWaitingInd()
 - cstaQueryDoNotDisturb()
 - cstaQueryForwarding()
 - cstaQueryAgentState()
 - cstaQueryLastNumber()
 - cstaQueryDeviceInfo()
 - attQueryACDSplit()
 - attQueryAgentLogin()
 - attQueryDeviceName()
- For AE Services 6.1, the OAM page for administering certain Tlink settings has been changed from "Security | Security Database | Tlinks" to "AE Services | TSAPI | TSAPI Links | Edit Link | Advanced Settings".

- AE Services 5.2 introduced a problem where certain fields in the subsequent CSTA Delivered event were incorrect after using the Route Select service to route a call to an external number. This issue has been resolved.
- The TSAPI Service now uses less TSDI memory when processing escape service requests.
- AE Services 5.2.2 introduced a problem where certain transfer and call park scenarios would cause the TSAPI Service to restart. This issue has been resolved.
- Prior to AE Services 6.1, the TSAPI Service might produce a core file when the system time was changed by more than five minutes.
- Prior to AE Services 6.1, the TSAPI Service might produce a core file if applications repeatedly tried to open more than 2500 streams.
- Prior to AE Services 6.1, the TSAPI Service might produce a core dump file on a System Platform offer after the initial installation.
- Prior to AE Services 6.1, the TSAPI Service did not always process requests on a stream in the order in which they were received.
- Prior to AE Services 6.1, the TSAPI Service did not always provide the correct device ID type for the routeUsed parameter in a CSTA Route Used event.
- Prior to AE Services 4.2.4, AE Services 5.2.1, and AE Services 6.1, the TSAPI Service did not always report the correct event cause in the CSTA Retrieved event. In some scenarios involving Service Observing, the TSAPI Service would report that the event cause was EC_PARK when it should have been EC_SILENT_MONITOR.
- Prior to AE Services 6.1, in some scenarios where a call traverses multiple vectors, the TSAPI Service did not always report the correct Vector Directory Number (VDN) as the distributing device in the private data associated with the CSTA Established event.
- Prior to AE Services 4.2.4, AE Services 5.2.2, and AE Services 6.1, the value of the acdSplit field in the private data accompanying a CSTA Delivered event was not always consistent with the value reported by Avaya Communication Manager.

- Prior to AE Services 5.2.2 and AE Services 6.1, in some call scenarios where a station is service observing a Vector Directory Number (VDN), the TSAPI Service would report the service observer as the last redirection device in the CSTA Delivered event.
- Prior to AE Services 6.1, if an application opened a stream with private data version 1-5, the private data accompanying a CSTA Originated event was actually for private data versions 6-8.
- Logic for setting the addedParty field in the CSTA Conferenced event has been changed for scenarios where another party on the call has the same extension number as the added party. Previously, the TSAPI Service would frequently provide a dynamic device identifier for the addedParty in these scenarios. Now the TSAPI Service is more likely to provide a static device identifier for the addedParty.
- Logic for setting the transferredDevice field in the CSTA Transferred event has been improved in scenarios where the call is transferred to an external party over a SIP trunk.
- Prior to AE Services 4.2.4, AE Services 5.2.2, and AE Services 6.1, if a TSAPI application invoked the CSTA Snapshot Call service for a call with more than 20 parties, the request would fail with CSTA error GENERIC OPERATION REJECTION. The request no longer fails, though only the first 20 parties are provided in the CSTA Snapshot Call confirmation event.
- Prior to AE Services 6.1, in some scenarios where a call visited multiple coverage points, the TSAPI Service might provide a CSTA Delivered event when the call alerted at each coverage point, but did not always provide a CSTA Diverted event when the call moved on to the next coverage point.
- Prior to AE Services 5.2.2 and AE Services 6.1, in some call scenarios where an ACD split had been conferenced onto a call and the conference originator then dropped off the call, the TSAPI Service would provide a CSTA Connection Cleared event indicating that the ACD split was no longer a party on the call.
- Prior to AE Services 6.1, the TSAPI Service would report extra events in some single step transfer call scenarios where the call had been routed to an agent before being transferred.
- Prior to AE Services 6.1, in some scenarios involving service observing and single step transfer, the TSAPI Service did not always provide the correct value for the calling device in the CSTA Delivered event.

- Prior to AE Services 6.1, in some call scenarios, after transferring a call with the single step transfer call service, the same call could not be transferred a second time with the single step transfer call service. The service would fail with error RESOURCE BUSY.
- Prior to AE Services 6.1, in some scenarios the TSAPI Service did not always provide the correct field values in CSTA Conferenced and Transferred events. These scenarios include:
 - A party was added to a call via the TSAPI single step conference call service, and the resulting call was involved in a subsequent conference or transfer operation.
 - A service observer joined a call, and the resulting call was involved in a subsequent conference or transfer operation.
- Prior to AE Services 6.1, in some call scenarios the TSAPI Service did not always provide the correct CSTA Connection Cleared events when a queued call left the queue. This problem could occur if the TSAPI application was not using the latest private data version.
- Prior to AE Services 5.2.1 and AE Services 6.1, the TSAPI Route Select service would fail with error VALUE OUT OF RANGE if the private data accompanying the service request had been formatted using the attV6RouteSelect() function but the application had opened the stream with private data version 7 or later.
- Prior to AE Services 6.1, in some call scenarios where a call is alerting at bridged appearances, the TSAPI Service would create ASAI domain controls for the stations with the bridged appearances, but did not relinquish all of those ASAI domain controls when the call terminates.
- Logic for taking the TSAPI Service offline has been corrected.
- Prior to AE Services 6.1, if a TSAPI application was terminated while it had many outstanding requests, the TSAPI Service would log a critical error describing a semaphore/queue inconsistency. For AE Services 6.1, the likelihood of these errors being logged is significantly reduced.
- Prior to AE Services 6.1, the TSAPI Service would log some OpenSSL errors as errno 336151548 or 336195711. The TSAPI Service now recognizes these values as OpenSSL errors and logs an appropriate error message.
- TSAPI message tracing for the Send DTMF Tones service has been improved. Previously, only the first 12 digits of the request appeared in the trace message.

- Prior to AE Services 6.1, the TSAPI Service would generate a warning ("g3_version 24 is not supported; substituting g3_version 23") when initializing a Tlink for a CM 6.x switch connection.
- TSAPI Message tracing has been made more efficient.
- For AE Services 6.1, the number of warning messages logged by the TSAPI Service has been dramatically reduced when using the default log settings.
- Prior to AE Services 6.1, trace files created by the TSAPI Service were sometimes named incorrectly:
 - Instead of "csta_trace-129.trace.out", the CSTA trace file was sometimes named "appttrace-129.trace.out".
 - Instead of "audit_trace-130.trace.out", the TSAPI audit trace file was sometimes named "appttrace-130.trace.out".