AVAYA

Avaya Aura® Application Enablement Services R5.2.4 Server and Client Release Notes

Issue 1.4
May 2013

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Service Pack Release 5.2.4 and describes important notes and known issues.

SOFTWARE RELEASE VERSIONS

Application Enablement Services Application	File Name
Avaya Aura® Application Enablement Services 5.2.4 CVLAN Client Linux 32-bit	cvlan-client-linux-5.2-540.i386.rpm
Avaya Aura® Application Enablement Services 5.2.4 CVLAN Client MS Windows 32-bit	cvlan-client-win32-5.2-540.zip
Avaya Aura® Application Enablement Services 5.2.4 TSAPI Client Linux 32-bit	tsapi-client-linux-5.2-540.i388.rpm
Avaya Aura® Application Enablement Services 5.2.4 TSAPI Client MS Windows 32-bit	tsapi-client-win32-5.2-540.zip
Avaya Aura® Application Enablement Services 5.2.4 TSAPI SDK Linux 32-bit	tsapi-sdk-linux-5.2-540.i386.rpm
Avaya Aura® Application Enablement Services 5.2.4 TSAPI SDK MS Windows 32-bit	tsapi-sdk-win32-5.2-540.zip
Avaya Aura® Application Enablement Services 5.2.4 JTAPI SDK	jtapi-sdk-5.2.0.540.zip
Avaya Aura® Application Enablement Services 5.2.4 Web Service - System Management SDK	smssvc-sdk-5.2.4.60.zip
Avaya Aura® Application Enablement Services 5.2.4 DMCC .Net SDK 32-bit	dmcc-dotnet-sdk-5.2.4.44.zip
Avaya Aura® Application Enablement Services 5.2.4 Web Services - Telephony SDK 32-bit	telsvc-sdk-5.2.4.60.zip
Avaya Aura® Application Enablement Services 5.2.4 DMCC XML SDK 32-bit	cmapixml-sdk-5.2.4.60.zip
Avaya Aura® Application Enablement Services 5.2.4 DMCC Java SDK 32-bit	cmapijava-sdk-5.2.4.60.zip
Avaya Aura® Application Enablement Services 5.2.4 Software Only 32-bit - 700504567	700504567.iso
Avaya Aura® Application Enablement Services 5.2.4 Hardware Bundled Upgrade for S8510 - 700504566	700504566.iso
Avaya Aura® Application Enablement Services 5.2.4 on System Platform - 700504569	700504569.iso
Avaya Aura® System Platform Service Pack R6.0.3	vsp-6.0.3.0.3.iso
Avaya Aura® System Platform Patch R6.0.3.9.3	vsp-patch-6.0.3.9.3.noarch.rpm

Application Enablement Services Application	File Name
Avaya Aura® Application Entablement Services Product Management Information Bases (MIBs)	aesvcs-product-mibs-5.2.4.60.zip
Standard MIBs	standard-mibs-5.2.4.60.zip

IMPORTANT NOTES

- AE Services 5.2.4 supports Red Hat Enterprise Linux 5.0 Update 3.

- AE Services 5.2.4 is compatible with the following Bundled Servers:
  - IBM x306m (S8500C)
  - Dell 1950 (S8510)

- AE Services 5.2.4 on System Platform is compatible with the following Servers:
  - IBM x3550 M2 (S8800)
  - Dell R610 (4GB RAM, H200 RAID Controller, 2x146 GB HDDs)

- AE Services 5.2.4 on System Platform is compatible with the following versions of System Platform:
  - System Platform R6.0.3

- AE Services 5.2.4 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 5.2.4 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.X (S8300D, S8510, S8800)
  - Communication Manager 6.2 (S8300D, S8510, S8800)

- Communication Manager 6.2 is compatible with the following AE Services Releases:
  - AE Services 5.2.3 and 5.2.4
  - AE Services 6.2

- MAPD is NOT supported beginning with Communication Manager 5.0

Avaya SIP Endpoints Supported by AE Services							
				CM/ASM Pair			
Endpoint	**Administered as**	**Endpoint Firmware**	**AE Services Release**	**CM Version**	**ASM Version**	**General Telephony**	**Agent Features**
9620	9620SIP	2.6	5.2.4	6.2	6.2	yes	no
9640	9640SIP	2.6	5.2.4	6.2	6.2	yes	no
9640G	9640SIP	2.6	5.2.4	6.2	6.2	yes	no
9630G	9600SIP	2.6	5.2.4	6.2	6.2	yes	no
9650	9600SIP	2.6	5.2.4	6.2	6.2	yes	no
9608	9608SIPCC	6.2	5.2.4	6.2	6.2	yes	yes
9611	9611SIPCC	6.2	5.2.4	6.2	6.2	yes	yes
9621	9621SIPCC	6.2	5.2.4	6.2	6.2	yes	yes
9641	9641SIPCC	6.2	5.2.4	6.2	6.2	yes	yes

				CM/SES Pair			
Endpoint	**Administered as**	**Endpoint Firmware**	**AES Release**	**CM Version**	**SES Version**	**General Telephony**	**Agent Features**
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
16CC	4620SIPCC	SIP16CC_1_0_12_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 (ACW)
- Auxiliary (AUX) work
- Auto-In/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
08/2010	35	Service Pack R4.2.4
02/2011	20	General Availability R6.1
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
10/2012	114	Service Pack R5.2.4

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".

- **The AE Services Management Console may not be accessible after a high availability failover for the AE Services on System Platform offer**

  This issue will be noticeable when a system administrator attempts to access the AE Services Management Console. Instead of receiving the Management Console logon screen, an exception will be displayed in the user's browser. If this issue occurs, please execute the following steps to resolve the issue:

  1. Using SSH or PuTTY, login to the AE Services server.
  2. Using the su command, switch to the root user.
  3. Execute the command "**sbin/service tomcat5 restart**"
  4. Wait a couple of minutes to allow the tomcat service to initialize the servlets.
  5. Login to the AE Services Management Console.

- **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 the Management Console until the re-login.

- **CallVisor Local Area Network (CVLAN) and DEFINITY LAN Gateway (DLG) Services Do Not Display Online**

  If there are no CVLAN or DLG links administered, the CVLAN or 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 CVLAN or DLG link.

  This is desirable behavior because it stops CVLAN or 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.

- **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.

- **DLG Links**

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

- **Local WebLM Server Port Number**

  If AE Services 5.2.4 has been upgraded from an earlier release, the server may be configured to use port 443 for accessing the local WebLM server. Most AE Services customers will see improved WebLM performance if the port number is changed from 443 to 8443. Note that this only applies to those AE Services installations that are using the local WebLM - that is, when the WebLM server is running on the same server or virtual machine as the rest of AE Services. If the installation is using a remote WebLM (one running on different server hardware or in a different virtual machine) then this note does not apply.

  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. On the "WebLM Server Address" page, if the value of the "WebLM IP Address" is not "127.0.0.1", then you are not using the local WebLM and this note does not apply to your installation. You may safely skip the rest of this procedure.

4. If the value of the "WebLM IP Address" is "127.0.0.1", change the value of the "WebLM Port" to 8443, ensure that the "SSL" box is checked and click on "Apply Changes".
5. When the confirmation screen is displayed, click on "Apply".
6. If your AE Services installation is a "Software-Only" offer, skip steps 7 & 8 and continue with step 9 to restart AE Services.
7. If your AE Services installation is either a "Bundled" offer or an "AE Services on System Platform" offer, you need to ensure that the firewall will allow port 8443 to be accessed. To do this, select “Security | Standard Reserved Ports”.
8. On the "Standard Reserved Ports" page, if the row: “TOMCAT HTTPS | 8443 | tcp” is not checked, then check it and click “Apply”.
9. After changing the WebLM Port to 8443, restart AE Services.
10. Select "Maintenance | Service Controller".
11. On the "Service Controller" page, click on the "Restart AE Server" button.
12. When the confirmation screen is displayed, click on "Restart".
13. Once the AE Services Server has restarted, this procedure is complete.

- **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 Authorization 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 boxes for the TSAPI, Transport Layer, ASAI Link Manager, DLG and 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 boxes for the TSAPI, Transport Layer, ASAI Link Manager, DLG and 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 https://downloads.avaya.com/css/P8/documents/100127799

- **Reserving Telephony Services Application Programming Interface (TSAPI) User Licenses**
  After installing or upgrading to AE Services 5.2, 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.

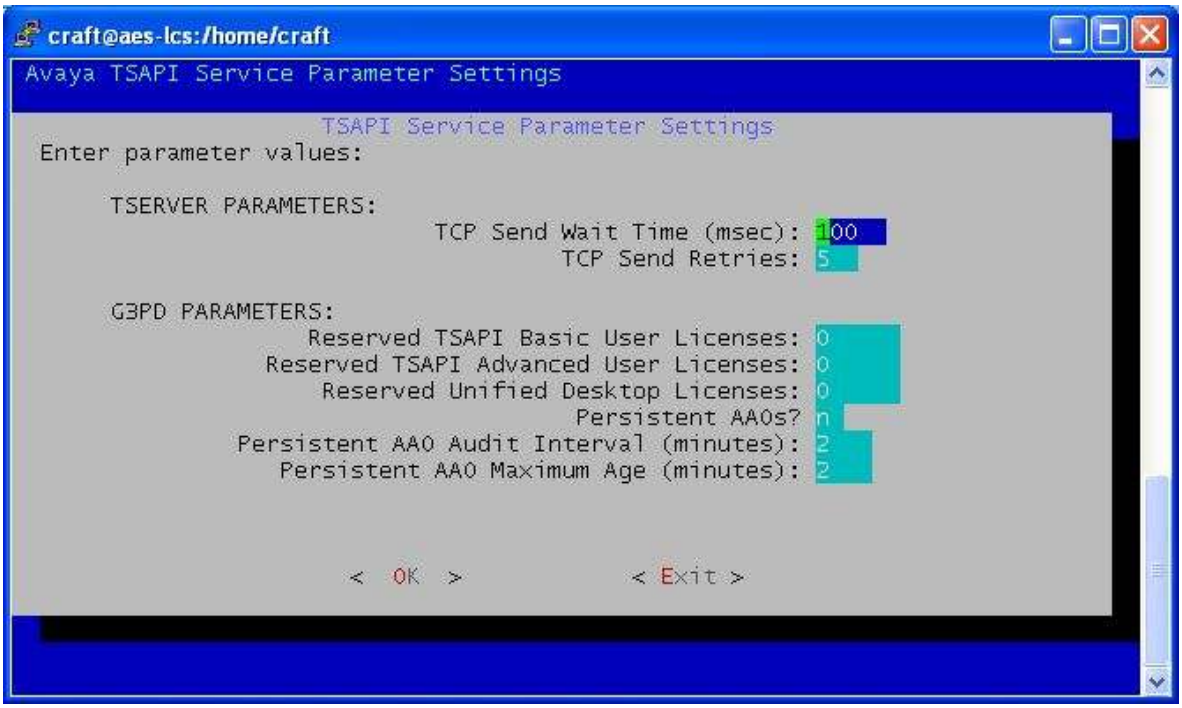
2. Log into the Application Enablement Services Management Console and select "Licensing | WebLM Server Access" to access the WebLM Logon screen. (The WebLM Logon screen should be displayed in a new browser window.)

3. Log into WebLM and select "Application_Enablement" to display the AE Services licensed features.

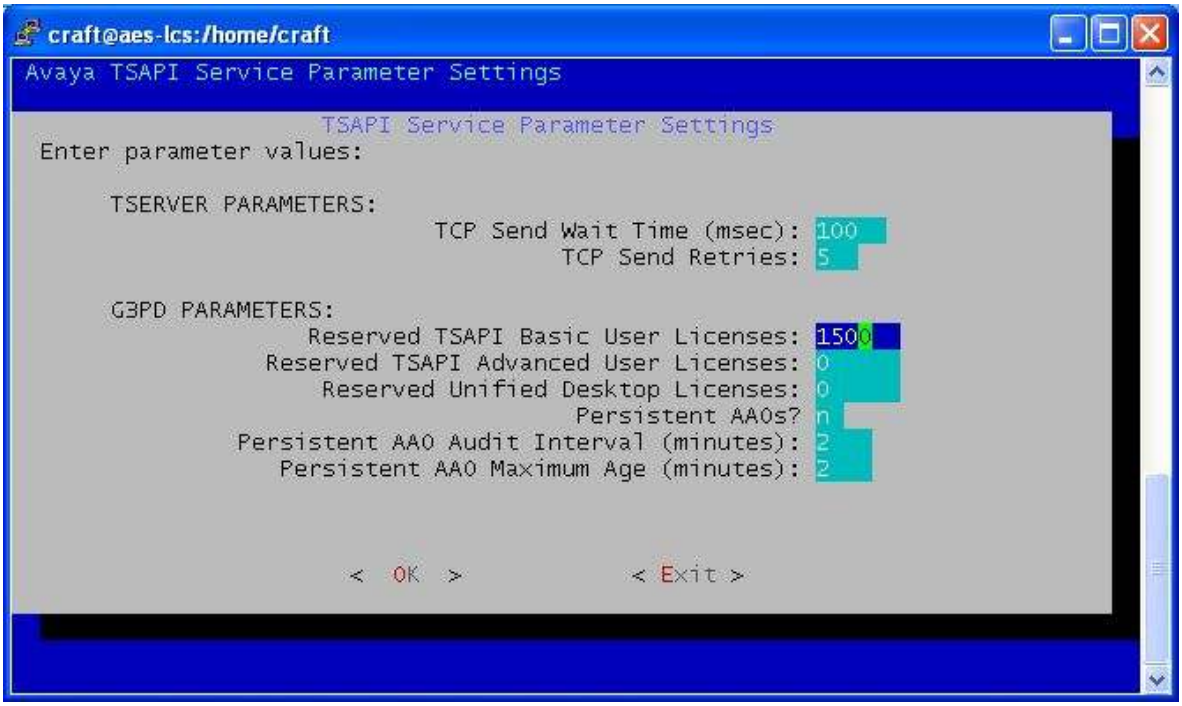
4. Note the number of TSAPI Simultaneous Users (VALUE_TSAPI_USERS) that are licensed.

5. Log into your AE Services server with root permissions and enter the following command to open the TSAPI Service Parameter Settings utility:
   `/opt/mvap/bin/tsapiparam.sh`

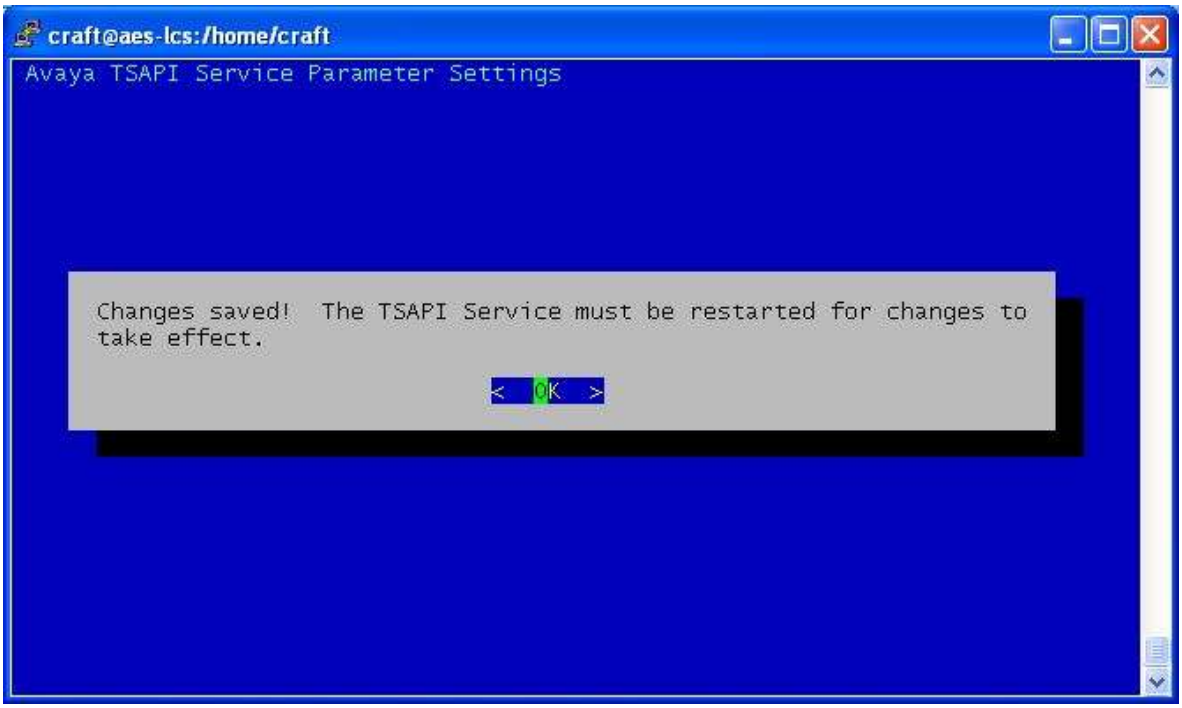
   The following screen will be displayed:



6. Use the up and down arrow keys to navigate to the "Reserved TSAPI Basic User Licenses" field, and enter the value that you recorded in Step 4 above. For example:



7. Use the tab key to highlight "OK" and press the Enter key. The following screen will be displayed:



8. Press the Enter key again to acknowledge that you have read this message and return to the main screen.

9. Use the tab key to highlight "Exit" and press the Enter key to exit the TSAPI Service Parameter Settings utility.

10. Log back into the AE Services Management Console and select "Maintenance | Service Controller".

11. 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.

  Follow these steps to enable Telephony Conferencing.
  1. From your browser, open http://ctisametime.lzt4aes.com/stcenter.nsf
  2. Click “Administer the Server” on the bottom right of the page.
  3. Log on by entering the name “sametime admin” and the password “cti123”.
  4. In the Administer the server page, select “Configuration | Meeting Services” and click the checkbox for “Allow people to schedule a telephone conference call for a web conference”. A telephony service provider is required.
  5. Select “Policies | Sametime Default Policy | Community Services” and click the checkbox for “Allow telephony for contact list, instant messaging, and instant meetings”.
  6. Reboot the Sametime Server.

  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.

- **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 Communication Manager 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.

  - 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 Call service does not work reliably for SIP stations.

  - User classified call does not generate an ALERTING event over an Adjunct Switch Application Interface (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 <u>all three</u> 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 R6.0.3 release notes at https://downloads.avaya.com/css/P8/documents/100127064

RESOLVED ISSUES IN AE SERVICES RELEASE 5.2.4

- **AE Services Server**
  - Previously, after an AE Services server failover, the non-TTS registered DMCC endpoints could not be recovered. This was the normal expectation; however, the client should receive a “TerminalUnregisteredEvent” for each endpoint that is not recovered. Under some circumstances, the “TerminalUnregisteredEvents” may be missing. This issue has been resolved.

  - While upgrading System Platform (AE Services on System Platform server) or the Hardware Bundled Upgrade for the S8510, the AE Services server reported “Application Enablement Service in not licensed in the license file” even when the license file was installed.

- **Device Media Call Control (DMCC) Service**
  - Previously, if the TSAPI or DMCC service is restarted, all logged in OC users are logged out and depending on the customer configuration, it could take a long time for all OC users to log back into AE Services. In AE Services 5.2.4, OC users are successfully logged back into AES in a few minutes.

  - Resolved an intermittent button press problem. The dialed digits sent by the client were not being transmitted from AE Services to the switch in certain situations (notably, when the Q931 signaling channel between AE Services and the switch was down). This fix ensures that the digits are transmitted to the switch correctly.

  - Second off-hook was not sent to a client when the station was using a headset. If a phone was initially on-hook and in headset mode, the client did not get a switch-hook event the first time that a call was initiated. This was due to multiple off-hook indications from the switch to the client application being flagged as duplicates, and being filtered out by AE Services. This case showed that it was not always prudent to filter out possible duplicate events. This fix allows the customer to decide if duplicate switch-hook events should be filtered out by AE Services, or not. This behavior is controlled via an option in the "/opt/mvap/conf/user-configuration.properties" file on the AE Services server.

  - Corrected formatting issues connected with displaying the DMCC Javadoc in a standard web browser.

  - The media stream was not redirecting to new IP port when using the RedirectMedia Request. This fix addresses a limitation in Communication Manager regarding the use of the RedirectMedia Request from DMCC clients. The DMCC Javadoc on the RedirectMedia Request have been annotated to explain the issue and to suggest a workaround.

- An audio interruption occurred every minute in server media mode. This issue arose when checking the sequence numbers in the RTP header of the media stream. This caused the audio output to appear stuttered and broken.

- Agent information in GetCallInformation Request was not provided if a service observer is involved in the call.

- Resolved an issue where a station was inadvertently unregistered because a software timer had not been cancelled at the appropriate moment.

- **Security**
  - The following Red Hat Linux security issues have been incorporated into Service Pack Release 5.2.4:
    1. RHSA-2012:0007-01 - Important: kernel security bug fix and enhancement update
    2. RHSA-2012:0017-01 - Important: libxml2 security update
    3. RHSA-2011:0472-01 - Important: nss security update
    4. RHSA-2011:0833-01 - Important: kernel security and bug fix update
    5. RHSA-2011:0927-01 - Important: kernel security and bug fix update
    6. RHSA-2011:1065-01 - Important: RHEL 5.7 kernel security and bug fix update
    7. RHSA-2011:1245-01 - Important: httpd security update
    8. RHSA-2011:1349-01 - Important: rpm security update
    9. RHSA-2011:0918-01 - Moderate: curl security update
    10. RHSA-2011:1377-01 - Moderate: postgresql security update
    11. RHSA-2011:1797-01 - Moderate perl security update
    12. RHSA-2011:0844-01 – Low apr security update
    13. RHSA-2011:1005-01 - Low: sysstat security, bug fix and enhancement update
    14. RHSA-2011:1073-01 – Low: bash security, bug fix and enhancement update

  - Postgresql Security Update CVE-2011-2483, Severity – Low
    "This update includes a security fix for crypt_blowfish before 1.1, as used in PostgreSQL before 8.4.9, as it does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash. The contrib/pg_crypto's blowfish encryption code could give wrong results on platforms where a signed character is used (which is most), may lead to encrypted passwords being weaker than they should be."

  - Apache Tomcat Information Disclosure CVE-2011-2204, Severity – Low
    "When using the MemoryUserDatabase (based on tomcat-users.xml) and creating users via JMX, an exception during the user creation process may trigger an error message in the JMX client that includes the user's password. This error message is also written to the Tomcat logs. User passwords are

visible to administrators with JMX access and/or administrators with read access to the tomcat-users.xml file. Users that do not have these permissions but are able to read log files may be able to discover a user's password."

- Oracle Java Critical Update Combined CVEs
  - CVE: CVE-2011-0862
    Component: Java Runtime Environment
    Sub-Component: 2D
    Last Affected Patch set: 6 Update 25 and before, 5.0 Update 29 and before, 1.4.2_31 and before

  - CVE: CVE-2011-0873
    Component: Java Runtime Environment
    Sub-Component: 2D
    Last Affected Patch set: 6 Update 25 and before, and 5.0 Update 29 and before

  - CVE: CVE-2011-0802
    Component: Java Runtime Environment
    Sub-Component: Sound
    Last Affected Patch set: 6 Update 25 and before, 5.0 Update 29 and before, 1.4.2_31 and before

  - CVE: CVE-2011-0814
    Component: Java Runtime Environment
    Sub-Component: Sound
    Last Affected Patch set: 6 Update 25 and before, 5.0 Update 29 and before, 1.4.2_31 and before

  - CVE: CVE-2011-0868
    Component: Java Runtime Environment
    Sub-Component: 2D
    Last Affected Patch set: 6 Update 25 and before

  - CVE: CVE-2011-0872
    Component: Java Runtime Environment
    Sub-Component: NIO
    Last Affected Patch set: 6 Update 25 and before, 5.0 Update 29 and before, 1.4.2_31 and before for Windows

- **TSAPI Client Libraries and SDKs**
  - Prior to AE Services 5.2.4, the TSAPI Windows Client library could stop processing messages for a stream opened using an encrypted Tlink, eventually causing the stream to fail.

  - 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 Certificate Authority certificate file that is installed with the TSAPI Client has been updated to include an additional Avaya CA certificate for establishing secure connections to the AE Services server.

- **TSAPI Service**
  - Prior to AE Services 5.2.4, if an application attempts to place a Service Observer on hold, the request will fail with CSTA error OUTSTANDING REQUEST LIMIT EXCEEDED. Beginning with AE Services 5.2.4, the request will fail with CSTA error PRIVILEGE VIOLATION ON SPECIFIED DEVICE.

  - Beginning with AE Services 5.2.4 and 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.)

  - Previously, 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. After the buffer overrun occurred, the TSAPI Service was likely to run out of TDI buffers and eventually crash.

  - Prior to AE Services 5.2.4, the TSAPI Service could crash while processing a CSTA Network Reached event resulting from a Single Step Transfer Call service request.

  - Previously, 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 5.2.4, 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.

A second issue remains unresolved with respect to this scenario: If there are no other active route registrations for the Tlink at the time that the application re-registers as the routing application, then even though the application receives a CSTA Route Register Req Confirmation event, it will NOT be registered as the routing application for the device. Applications that register as the routing application for two or more devices should not encounter this issue.

- Prior to AE Services 5.2.4, 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.

- Previously, the TSAPI Service did not provide the correct sequence of CSTA Unsolicited events for calls that were treated by a converse vector step.

- Prior to AE Services 5.2.4, the TSAPI Service did not provide consistent field values in CSTA Unsolicited events for Automatic Callback Call scenarios where the called party was a local station extension.

- Previously, 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 5.2.4, the TSAPI Service did not always set the clearedCall parameter of the CSTA Call Cleared event correctly. Beginning with AE Services 5.2.4, the device ID for the cleared call is always set to “0”, and the device ID type is always set to DYNAMIC ID.

- Previously, the Single Step Transfer Call service did not release all of its resources in some failure scenarios where the transfer destination is busy or invalid. As a result, subsequent attempts to invoke the Single Step Transfer Call service could fail with error RESOURCE BUSY.

- Prior to AE Services 5.2.4, 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 5.2.4, this problem has been fixed.

- In prior releases, the TSAPI Service could stop processing requests for a station if an application issued a Consultation Call service request for the station immediately after issuing a Hold Call service request for the station.

- Prior to AE Services 5.2.4, 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 CSTA Make Call service request). Beginning with AE Services 5.2.4, private data will no longer accompany the CSTA Service Initiated event in this scenario.

- Previously, for private data versions 5 and later, the TSAPI Service may not provide the correct Universal Call ID (UCID) or distributing device in the private data accompanying a CSTA Established event. This problem was most likely to occur in CSTA Established events resulting from a Single Step Conference Call service request.

- Prior to AE Services 5.2.4, 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.

- In prior releases, the TSAPI Service did not provide the correct device ID type for the agentDevice parameter in the CSTA Logged On and Logged Off events if the extension number of the agent device contained seven or more digits.

- Prior to AE Services 5.2.4, the TSAPI Service did not always provide the correct device ID type for the calledDevice parameter in the CSTA Originated event. This problem was most likely to occur if the extension number of the called device contained seven or more digits.

- Previously, 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 5.2.4, in some cases the TSAPI Service would provide the wrong device ID type (STATIC ID instead of DYNAMIC ID) for the dropped connection in a CSTA Connection Cleared event.

- In prior releases, 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 5.2.4, the TSAPI Service did not always report the correct value for Total TSDI Memory in Use. (This value can be viewed through the AE Services Management Console by selecting “Status | Status and Control | TSAPI Service Summary” and then clicking the “TSAPI Service Status” button.)

- Previously, the g3peek utility’s AAO Information Output screen did not display the correct age of Call Control ASAI Association Objects.

- The g3trace output format for ATT Query Device Info Confirmation events has been corrected.