# R4.1 Application Enablement Services Software Only Server, Bundled Server and Client Release Notes – GA Release

**December 2007**

## INTRODUCTION

This document introduces the GA release information of Application Enablement (AE) Services Release 4.1, and describes important notes and known issues. The *Avaya MultiVantage Application Enablement Services Overview* has all the new release information but some of the highlights are:

**Dial Plan Expansion (including Call Information Services support)**
- Support of 13-digit dial plan

**Integration with Microsoft**
- Support for OCS 2007
- Support for Agent Login ID

**SMS Licensing**

**Duplication Improvements**
- IP Station Failover

**Security Improvements**
- TSAPI/JTAPI/CVLAN Clients Secure Application Links
- Audit Trails of OAM Activity
- Password management
- Role-based access control (RBAC)
- Various certificate enhancements
- DMCC Authorization Checks of CSTA Service Request
- DMCC and OCS/LCS Integration host authorization and authentication

**Platform Enhancements**
- Support Command Line Interface for Alarming

**API Support for 508 Compliance**
- Send/Receive TTY via applications

**Call Control Clients Enhancements**
- TSAPI/JTAPI Alternate Tlink Selection

TSAPI/JTAPI support for Single Step Transfer
TSAPI/JTAPI/CVLAN Heartbeats
TSAPI/JTAPI/CVLAN support for unsolicited Call Forwarding and Do Not Disturb (DND)/Send All Calls (SAC) Events
JTAPI FastConnect
Microsoft Vista Support
TSAPI/JTAPI Enhanced VDN Monitoring for Predictive Calls

**DMCC Enhancements**

Expanded Call Control Services support
.NET/C# SDK
Session Management for Devices for N+1 duplication
Media forking from telephone to application

## SOFTWARE RELEASE ISO VERSIONS

| Application | ISO Version |
|---|---|
| **Server Bundled & SW-Only** | ISO 31-2 |
| **JTAPI Client/SDK** | 4.1.13 |
| **TSAPI Client/SDK** | 4.1.12 |
| **CVLAN Client** | 4.1.14 |
| **Telephony Web Services SDK** | 4.1.0.589 |
| **DMCC Java SDK** | 4.1.0.589 |
| **DMCC XML SDK** | 4.1.0.596 |
| **SMS SDK** | 4.1.0.589 |
| **DMCC .NET SDK** | 4.1.234 |

## SOFTWARE RELEASE FILE NAMES

| Application | Files Name |
|---|---|
| **Application Enablement Services CVLAN Client Linux** | cvlan-client-linux-4.1-330.i386.rpm |
| **Application Enablement Services CVLAN Client Windows** | cvlan-client-win32-4.1-330.zip |
| **Application Enablement Services IPCommunications SDK (Device and Media Control/DMCC)(Java)** | cmapijava-sdk-4.1.0.589.zip |
| **Application Enablement Services IPCommunications SDK (Device and Media Control/DMCC)(XML)** | cmapixml-sdk-4.1.0.596.zip |
| **Application Enablement Services IPCommunications SDK (System** | smssvc-sdk-4.1.0.589.zip |

| | |
|---|---|
| **Management Services)** | |
| **Application Enablement Services IPCommunications SDK DMCC dotnet SDK** | dmcc-dotnet-sdk-4.1.234.zip |
| **Application Enablement Services IPCommunications SDK Telephony Services** | telsvc-sdk-4.1.0.589.zip |
| **Application Enablement Services JTAPI MS Windows 32-BIT Client** | jtapi-client-win32-4.1-323.zip |
| **Application Enablement Services JTAPI MS Windows SDK** | jtapi-sdk-win32-4.1-323.zip |
| **Application Enablement Services JTAPI OS Independent Client** | jtapi-client-osindependent-4.1-323.zip |
| **Application Enablement Services JTAPI OS Independent SDK** | jtapi-sdk-osindependent-4.1-323.zip |
| **Application Enablement Services TSAPI Client Linux** | tsapi-client-linux-4.1-323.i386.rpm |
| **Application Enablement Services TSAPI Client MS Windows** | tsapi-client-win32-4.1-323.zip |

## IMPORTANT NOTES

This release of the AE Services is compatible with Communication Manager 3.0, 3.1, 4.0 and 5.0. Not all features are supported by all releases of CM.

Release History:

| Date | Build | Change(s) |
|---|---|---|
| 3/07 | 47-3 | General Availability R4.0 |
| 6/07 | 50-1 | General Availability R4.0.1 |
| 12/07 | 31-2 | General Availability R4.1 |

## KNOWN ISSUES AND WORKAROUNDS

- **Database Workaround For AE Services 4.1 Builds Prior to 28**

Sw-Only and Bundled - Database Upgrade - Use this workaround if you are upgrading from a previous 4.1 load that is prior to build 28. Run this workaround before upgrading to the General Availability load.

1. Download this script file **workaround.sh** to /tmp on your AES server.
2. Login as root/sroot
3. $chmod 777 /tmp/workaround.sh

4. $su avaya
5. $/tmp/workaround.sh <build number of the load currently on the machine>
6. $su root or sroot
7. $/sbin/service mvap restart

- **Upgrading with User Installed Certificates from AES 4.0 to AES 4.1**

The following are required manual workaround steps for an AES 4.0 to AES 4.1 upgrade in which the user has installed a server certificate, especially for LCS users.

1. Before the upgrade process is invoked, the Backup process must be executed using the OAM screen “CTI OAM -> Maintenance -> Backup Database”. Save the tar file to a safe location which will not be affected by the upgrade.

2. Remove the server certificate using the OAM screen “CTI OAM -> Administration -> Certificate Management -> Server Certificate”. Select the checkbox next to the server certificate and click the Delete button. In the pop-up window, confirm the deletion. (Note: The server certificate is preserved in the Backup image.)

3. Perform the AES 4.0.x to AES 4.1 upgrade.

4. Restore the Backup image using the OAM screen “CTI OAM -> Maintenance -> Restore Database”.

5. Once the restore completes successfully, verify the server certificate was restored using the OAM screen “CTI OAM -> Administration -> Certificate Management -> Server Certificate”.

6. Restart the AE Server or restart the Web Server using the OAM screen “CTI OAM -> Maintenance -> Service Controller” by selecting the “Restart Web Server” button.

- **Known 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 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 work around 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 CM does not have a crossfire 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 CM does not have a crossfire 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.

- Attempting Single Step Transfer with SIP stations will result in unpredictable behavior. It is not supported at this time.

- DTMF Tones are not supported on SIP endpoints.

## • AE Services Upgrades – Please reference the Installation Manual for all upgrades

- For the **Software Only Offer**, please note the following:
  The Apache (httpd) service must be restarted after an upgrade.

- For 3.0 to 4.1 upgrades, please perform the necessary steps to manually backup and restore the User Services database (LDAP) as listed in the Installation Manual in order to maintain a synchronized LDAP and Postgres database.

- For **Software Only Offer** 4.0.1 to 4.1 upgrades, be sure to perform the backup of the database. The database backup preserves the license file. The license file will be restored when the database restore is completed.

- Upgrades will fail after three installs – Applies only to the Bundled Offer
  The Installer allows a maximum of three upgrades. The fourth upgrade will fail. The workaround for this is documented in the Installation Guide for the Bundled Server.

## • Setting DEFAULT CLOCK To TSC In SW-ONLY OFFER

The default clock was changed to pmtmr (power management timer) from RHEL 4 update 4, which caused the time() system call to take longer to complete, which in turn can cause AES performance degradation. The Section titled "Optimizing the Linux software for AE Services" in Chapter 2 of the Software-Only Installation Guide describes the procedure for configuring your system to use the recommended clock.

- **CVLAN Windows Client Workaround**

Before installing the CVLAN client check {Windows Directory}\system32 for the presence of DLLs **libeay32.dll** and **ssleay32.dll**. If they are present backup these files and perform the CVLAN install as directed. Once installed, if your application displays an error message, copy the saved DLLs back into the system32 directory.

- **HTTP Issue**

When attempting to access the OAM pages, you are automatically switched to use https instead of the regular insecure http protocol. This may cause a problem in which the user is denied access to the tomcat server. The user will see the following error message:

Access Denied (connect_method_denied)

Your request attempted a CONNECT to a port "8443" that is not permitted by default.
This is typically caused by an HTTPS URL that uses a port other than the default of 443.
For assistance, contact your network support team.

**Solution:**
In order to resolve this issue, the user must turn off the browser's proxy settings or include the IP address or the DNS name of the AE Services server in the "Proxy Exception's box".

For IE 6 users, click on "Tools -> Internet Option -> Connections -> LAN Settings -> Advanced". In the "Exception box", enter the full IP address or the DNS root (which ever you use) of the AE Services server.

For Firefox users, click on "Tools -> Options -> General -> Connection Settings" (for Linux version, click on "Edit -> Preferences -> General -> Connection Settings"). In the "No proxy For" box, enter the full IP address or the DNS root (which ever you use) of the AE Services server.

For Mozilla users, your exception box is in the following location: "Edit -> Preferences -> Advanced -> Proxies". "). In the "No proxy For" box, enter the full IP address or the DNS root (which ever you use) of the AE Services server.

- **Process to Change the Server IP Address**

If the IP address of an AE Services server is changed without stopping the server or if the IP address is changed and then an attempt is made to set the new address through the web pages without stopping the server service (which is using the connection), an error message will be displayed. The error message will appear on the Local IP web page and indicate that the database entry for the IP address does not match the IP address configured on the server. The proper procedure to change the IP address is as follows:

1. Log on as root/sroot at the AE Services Linux console

2. Issue the following:
   service mvap stop

3. Update /etc/hosts file with the new IP address

4. Update CTI OAM > Administration > Local IP with the new IP address. The page should be submitted even if it shows "ANY".

5. Issue the following:
   service mvap start

- **Customer-Administered Server Certificate Expiration**

The AES administration pages do not currently support the installation of a renewed certificate to replace an expiring certificate. Instead, when a certificate will be expiring soon, it will be necessary to request a new certificate. Upon receipt of that new certificate, it should be installed on the AES system using the OAM pages, and the old certificate should be deleted. Additionally, the old certificate should be revoked on your Certificate Authority.

If a certificate expires before it can be replaced, the OAM will no longer list the installed certificates because of a date validation failure. Please contact Avaya Support for assistance with installing a new certificate if this happens.

- **Error Displayed on License File Loading**

After upgrading a SW-Only system from 3.X to 4.1 a file .##<Server>Application_Enablement.l was not cleaned up. When trying to install the license file an error message was displayed:

"*Error installing license. An error occurred while performing license installation checks. Please ensure that all the required steps were performed before deploying WebLM server."*

Change directory to the /var/tmp directory and look for the file as stated above. If it is there remove it. After manually removing the file .## file the license can then be loaded through WebLM.

- **Restart Tomcat**

After a fresh installation of AE Services and a restore of a previous database the WebLM page is not accessible. The license file could not be loaded. If this occurs at the system prompt issue:

service tomcat restart

WebLM should now be accessible and the license file can be loaded