R4.2.1 Application Enablement Services Software Only Server, Bundled Server and Client Release Notes

August 2008

INTRODUCTION

This document introduces the Generally Available release of the Application Enablement (AE) Services Release 4.2.1 and describes important notes and known issues. The *Avaya MultiVantage® Application Enablement Services Overview* has a complete list of 4.X features. This release introduces the following two enhancements for DMCC:

- **H.323 Signaling**
    - The "Traffic rate for applications" guidance for no Session and H.323 signaling encryption has been updated for the Dell 1950 server. The following is the new guidance: 400 simultaneous outstanding registrations with 10 simultaneous registrations per CLAN. When a registration completes successfully, a new one may be launched immediately until all required stations are registered.
- **Bridge Alert Configuration**
    - When administering AE Services for usage with Microsoft Office Live Communications Server a Bridged Alert Configuration (Bridged Alert Config) feature in AE Services OAM has been added to control the number of bridged appearances that appear on an assistant's desktop -- Microsoft Office Communicator will display a pop-up conversation window whenever a call appears for a bridged appearance. See section "*New Configuration Changes for Bridge Appearance Alert for Microsoft Office Live Communications"* in the release notes for details on how to administer this feature.
- **What's Changed In AES 4.2.1?**

AE Services 4.2.1 is a bug fix release for AE Services 4.0, 4.0.1, 4.1, and 4.2

AE Services 4.2.1 supports Red Hat Enterprise Linux 4.0 Update 6

AE Services 4.2.1 is compatible with the following Bundled Servers:

- IBM x306 (S8500B)
- IBM x306m (s8500c)
- Dell 1950

SOFTWARE RELEASE VERSIONS

Application	File Name
Application Enablement Services CVLAN Client Linux	cvlan-client-linux-4.2-338.i386.rpm
Application Enablement Services CVLAN Client Windows	cvlan-client-win32-4.2-338.zip
Application Enablement Services TSAPI Client Linux	tsapi-client-linux-4.2-338.i386.rpm
Application Enablement Services TSAPI Client MS Windows	tsapi-client-win32-4.2-338.zip
Application Enablement Services TSAPI SDK Linux	tsapi-sdk-linux-4.2-338.i386.rpm
Application Enablement Services TSAPI SDK MS Windows	tsapi-sdk-win32-4.2-338.zip
Application Enablement Services JTAPI OS Independent Client	jtapi-client-osindependent-4.2-338.zip
Application Enablement Services JTAPI OS Independent SDK	jtapi-sdk-osindependent-4.2-338.zip
Application Enablement Services JTAPI MS Windows 32-BIT Client	jtapi-client-win32-4.2-338.zip
Application Enablement Services JTAPI MS Windows SDK	jtapi-sdk-win32-4.2-338.zip
Application Enablement Services IPCommunications SDK (System Management Services)	smssvc-sdk-4.2.0.308.zip
Application Enablement Services IPCommunications SDK DMCC dotnet SDK	dmcc-dotnet-sdk-4.2.47.zip
Application Enablement Services IPCommunications SDK Telephony Services	telsvc-sdk-4.2.0.308.zip
Application Enablement Services IPCommunications SDK (Device and Media Control/DMCC)(XML)	cmapixml-sdk-4.2.0.247.zip
Application Enablement Services IPCommunications SDK (Device and Media Control/DMCC)(Java)	cmapijava-sdk-4.2.0.247.zip
Application Enablement Services Server Software for the Software Only Solution	swonly- r4-2-1-20-5-20080717.iso
Application Enablement Services Server Software for Bundled Solution	bundled-r4-2-1-20-5-20080717.iso

IMPORTANT NOTES

AE Services 4.2.1 is compatible with the following Communication Manager Releases and Platforms:

- CM 3.0 (G3csi, S8300, S8400, S8500, S87xx)
- CM 3.1.x (G3csi, S8300, S8400, S8500, S87xx)
- CM 4.x (S8300, S8400, S8500, S87xx)
- CM 5.0 (S8300, S8400, S8500, S87xx)

- CM 5.1 (S8300, S8400, S8500, S87xx)

Communication Manager 5.1 is compatible with the following AE Services Releases:

- AE Services 3.1.x
- AE Services 4.0, 4.01, and 4.1
- AE Services 4.2 and 4.2.1

Note: MAPD is NOT supported on CM 5.x

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
4/08	4.1.16	General Availability R4.1.1 JTAPI Client/SDK
5/08	19-4	General Availability R4.2

KNOWN ISSUES AND WORKAROUNDS

• 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 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 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.

- The Single Step Transfer service does not work reliably for SIP stations.

- DTMF Tones are not supported on SIP endpoints.

- User classified call does not generate an ALERTING event over 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 that the call is associated with.

• NIC Configurations Not Saved

In AE Services 3.x releases, the NIC configurations (auto negotiation, speed, and duplex) were not preserved in AE Services Database. Starting with AE Services 4.0, the NIC interface can be configured via Web OA&M page and the settings are stored in database. For those servers upgraded from 3.x, all the NIC interfaces have to be re-configured via Web OA&M page.

• TSAPI Clients Opening More Than 2500 Maximum Streams Can Result In New Monitors Not Being Created

If TSAPI clients try to open more than the maximum number of streams (2500), an error will be returned. This is proper behavior. However, certain resources are not freed as they should be. If the client applications continue attempt to connect and the resource is exhausted, then the TSAPI service will fail to create new monitors, to accept new connections (even after other streams are closed), and to update TSAPI OAM pages. This will happen after about 1500 such failed requests.

The following error log entry indicates that you have exceeded 2500 open streams:

```
ERROR:CRITICAL:TSAPI:TSERVER:DriverService.cpp/243 93
couldn't register with session manager
```

These error log entries indicate that the resource has been exhausted and the TSAPI service must be restarted:

```
ERROR:WARNING:
TSAPI:MVAPLicense::acquireTSAPIUsers:getNumAcquired
failed: Internal error:socket()
ERROR:CRITICAL:TSAPI:TSERVER:DriverService.cpp/229 93
accept failed 20 ERROR:WARNING:TsrvCmdUtility:main:Receive
from server failed rc= 0, errno= 2
ERROR:WARNING:TsrvCmdUtility:main:Receive from server
failed rc= -1, errno= 62
```

The TSAPI Service must be restarted to recover the abandoned file descriptors or AE Services must be rebooted

- ## WebLM Enterprise Model – Using HTTPS

  You will need to run this workaround if all three of the following conditions are true:

  1. Your master WebLM Server, which hosts the Enterprise License File (ELF), is not co-located with an AES Server,
  2. You have local WebLM servers that are co-located with AE Services
  3. You wish to use HTTPS for communication between the master and local WebLM Servers [for example, to push an Allocation License File (ALF) to a local WebLM server on AE Services].

  Locate the Enterprise Web Licensing WebLM Patch. The name of the file is ImportCertToWebLM.zip in the patch directory on the Bundled ISO and in the root directory of the SW-Only ISO.

  - Download importCertToWebLm.zip files to your EWL server.
  - Unzip the file
  - Follow the directions in the README to install

- ## WebLM Session May Hang

  - If you performed one of the following actions on WebLM the session may hang.
    - Repeatedly uninstall and install licenses
    - Repeatedly refreshing license page

    You should close the current session and open a new session

- **Server PAM Time Deny Function**

    - In the AES 4.2 Release, the PAM Time Deny function did not work correctly. This issue was resolved in the 4.1.2 release.

- **CVLAN Service Does Not Display Online**

    - If the AE Server has no CVLAN links administered, the Controller Status of CVLAN Service will appear as running under CTI-OAM home, but will appear as OFFLINE under the services summary. The service will appear as online after you add a CVLAN link.

- **DLG Service Does Not Display Online**

    - If the AE Server has no DLG links administered, the Controller Status of DLG Service will appear as running under CTI-OAM home, but will appear as OFFLINE under the services summary. The service will appear as online after you add a DLG link.

- **DLG Links**

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

- **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:

    For AES bundled server:

    1. Log in as sroot.
    2. Issue “service mvap stop”
    3. Execute “/opt/mvap/bin/netconfig” to bring up GUI.

4. Enter/Modify IP address(es) per NIC interface (Make sure “Enable” boxes are checked), and save/exit by “OK” button.
5. Re-login as sroot with new IP address if administering remotely. Issue “service network restart” (This step is pre-cautionary).
6. Log into OAM “AE Server Administration” using new IP address of AES server. (Note: If OAM web page is not responding in proper time, issue “service tomcat5 restart” and try again).
7. Go to “Administration” -> “Network Configuration” -> “Local IP” and set the new IP address(es) for all “Connectivity” entries.
8. Go to “Maintenance” -> “Service Controller” and apply “Restart AE Server” button.
9. Make sure all services are in “Running” state, and connection state to switch(es) is functional.

For AES Software-Only server:

For AES Software-Only server:

1. Log in as sroot.
2. Issue “/sbin/service mvap stop”
3. *** Customer is responsible for the change, but highly recommend using Linux utility such as /usr/bin/system-config-network if using Redhat Release 4. /etc/hosts file must be updated with new IP address(es). Issue “/sbin/service network restart” (This step is pre-cautionary). ***
4. Log into OAM “AE Server Administration” using new IP address of AES server. (Note: If OAM web page is not responding in proper time, issue “/sbin/service tomcat5 restart” and try again).
5. Go to “Administration” -> “Network Configuration” -> “Local IP” and set the new IP address(es) for all “Connectivity” entries.
6. Go to “Maintenance” -> “Service Controller” and apply “Restart AE Server” button.
7. Make sure all services are in “Running” state, and connection state to switch(es) is functional.

Note: If OAM page cannot be accessed, check status of httpd/tomcat5 processes by “/sbin/service httpd status” and “/sbin/service tomcat5 status”, and start if not running.

- **Sametime 7.5.1**

    - There is a defect in Sametime Connect 7.5.1 which prevents telephony presence changes form being displayed. Sametime Connect 8.0 does not exhibit this behavior.

Installation Notes

- **Sametime**

  AE Services supports integration with IBM Lotus Sametime Version 7.5.1 and 8.0. The following software from IBM is required. In addition, the Avaya AE Services Sametime zip file is needed to complete the installation and setup of this feature.

    - Lotus Sametime
        - Lotus Sametime Server 7.5.1 or 8.0 (Windows only)
        - Lotus Sametime Clients 7.5.1 or 8.0 (Windows, Linux, Mac OS X)
        - Lotus Sametime 8.0 SDK (Windows, Linux, Mac OS X) (works with 7.5.1 and 8.0 clients)

    - Avaya AES Sametime Integration
        - avaya-aes-sametime.zip can be downloaded from the following Web Site

  http://devconnect.avaya.com/AEServices_LotusSametime

  For complete installation and setup instructions, see the following document:

  Avaya Application Enablement Services
  Release 4.2
  Integration Guide for IBM Sametime

DELTA BUG FIXES

This section summarizes 4.X issues addressed in AE Services 4.2.1

The following issues have been resolved for DMCC.

- CM sends Lamp update messages for all buttons (administered or not) for a given station periodically, whether the lamp state has changed or not. AES filters lamp updates messages from CM, if the previous lamp state of the button is same as the new updated state. This filtering is done for only those buttons that are administered. AES was not filtering lamp updates if the button was not administered. Now AES filters redundant lamp update messages for un-administered buttons.

- If a Java client tries to get a reference to a service via getService() using two separate threads at the same time, client may get two instances of the services due to race condition, instead of one. All services are supposed to be singletons for a given Service Provider.

- There was a problem where the server was not properly filtering events based on the negotiated protocol version of the client. The server will now filter events that are not supported for a given protocol version. With this fix, clients will receive events supported by the protocol version they are running, and events supported in newer versions will not be published (sent) to clients running with an older protocol version than the AE Server.

- The FailedEvent will now return a cause value of “destNotObtainable” instead of “keyOperation” when an invalid extension number is dialed.

- The XML documentation for GetButtonIformationResponse was updated to clarify the device id returned in the response is in the format of an extension and not in a valid third party device id format.

- When attempting to register an extension in shared control mode while the base set was not logged-in, the client application received a response with an error code = -1 (instead of the 3009 that was expected). This fix corrects that problem and also slightly extends the possible error codes.

- When attempting to register an extension immediately following the start of the AE Server, the client application received a denial response. This was due to the fact that the DMCC License Service had not fully initialized by the time that the client sockets were opened (and the registration request was issued).

- Previously, when last member in Authorized hosts is deleted, the changes are not passed to lifecycle management.

The following issues have been resolved for JTAPI Client/SDK.

- Previously, when performing a transfer or conference operation, under certain conditions the JTAPI middleware might associate the wrong User To User Information with the call.

The following issues have been resolved for the Platform.

- AES fails to start if system has more than 4 GB RAM. The JVM has a limitation that can only support up to 2 GB for its maximum heap memory. The fix is to have AES allocated half of the system RAM size and up to 2 GB for the JVM heap memory.

The following issues have been resolved for the SMS.

- SMS clients were not receiving the complete array of data from the Button_Data_6 field of the Station model. This has been rectified and SMS should now properly receive the entire array.

- Previously SMS was improperly shutting down the ossicm proxy while it still had active SAT connections. This was believed to be the cause of what appeared to be hanging SAT connection on CM. SMS no longer shuts down the ossicm due to a login failure if there are still active SAT connections.

- SMS now attaches the name of the machine acquiring a license from WebLM in the process name. This should be useful to those whom are utilizing Enterprise Wide Licensing.

- Previously clients were not able to see devices that were registered in shared control mode via the RegisteredIPStations model. The required fid's have now been added to properly view these devices via the RegisteredIPStations model.

The following issues have been resolved concerning the CVLAN Client

- Beginning with Release 4.1.0, the installation program for the AE Services TSAPI and CVLAN Windows clients began to install the OpenSSL Dynamically Linked Libraries (DLLs) libeay32.dll and ssleay32.dll in the Windows system32 folder. Unfortunately, the version of the installed DLLs was sometimes incompatible with other Windows applications using OpenSSL.
  To address this issue, these DLLs have been renamed as aes-libeay32.dll and aes-ssleay32.dll and are now installed in \windows\system32.

The following issues have been resolved concerning the CVLAN

- Previously, CVLAN would sometimes start without acquiring the VALUE_CVLAN_ASAI license. Now, it does.

- Previously, the CVLAN service did not wait for WebLM to come up before starting and were taken offline when WebLM was not available. Now, they will wait up to 50 seconds for WebLM.

The following issues have been resolved for DLG.

- Previously, the DLG service did not wait for WebLM to come up before starting and were taken offline when WebLM was not available. Now, this service will wait up to 50 seconds for WebLM.

The following issues have been resolved concerning the Database.

- Previously, certain DB accesses at start-up could cause server crashes. Now, this does not happen.

The following issues have been resolved concerning TSAPI Client/SDK.

- Beginning with Release 4.1.0, the installation program for the AE Services TSAPI and CVLAN Windows clients began to install the OpenSSL Dynamically Linked Libraries (DLLs) libeay32.dll and ssleay32.dll in the Windows system32 folder. Unfortunately, the version of the installed DLLs was sometimes incompatible with other Windows applications using OpenSSL.
  To address this issue, these DLLs have been renamed as aes-libeay32.dll and aes-ssleay32.dll and are now installed in \windows\system32.

- If a host name resolution (for example, the Domain Name Service or DNS) is not properly configured on the AE Services server, it may take ten seconds or longer for a TSAPI application to open an ACS stream or for a JTAPI application to create a Provider. The TSAPI Service has been enhanced so that it no longer attempts to resolve Worktop IP Addresses to Host Names unless:

  - The TCP Preferred Naming Format for TSAPI is set to "Host Name", and
  - The Extended Worktop Access and/or Auto Admin of LAN Addresses features are enabled.

  Further, once the Host Name for a Worktop is set to "<unknown>", the TSAPI service will not make subsequent attempts to resolve the Host Name for that Worktop.

The following issues have been resolved concerning TSAPI Service Error Messages:

- Within the TSAPI Service, the format of the error message:

  [EVENT.CPP] cstaxeventmap - Connection list has more than 6 parties, but not over the limit.

  has been changed to:

  [EVENT.CPP:<AAO-ID>] CSTA Conferenced Event connection list for call ID <call-ID> contains more than 6 parties. (Number of parties=<number-of-parties>.

- Within the TSAPI Service, the format of the error message:

  [EVENT.CPP] cstaxeventmap - CCO is NULL, Cannot build Conference Event.

  has been changed to:

  [EVENT.CPP:<AAO-ID>] CCO not found for call ID <call-ID>; cannot build CSTA Conferenced Event.

- Within the TSAPI Service, the format of the error message:

[EVENT.CPP] cstaxeventmap() - Connection list overflow (more than 20 parties).

has been changed to:

[EVENT.CPP:<AAO-ID>] Detected connection list overflow (more than <party-limit> parties) while building CSTA Conferenced Event for call ID <call-ID>. (Number of parties=<number-of-parties>.)

- Within the TSAPI Service, the format of the error message:

  Found Kludged party. Set to Null state

  has been changed to:

  The PBX Driver has determined that device <device-string> is no longer an active party on call ID <call-ID>; setting that party's call state to CCO::Null.

- Within the TSAPI Service, the format of the error message:

  [UFAILURE.CPP]: AAO (id=0) cannot locate object [CAS:<session-ID>].

  has been changed to:

  [UFAILURE.CPP] The PBX driver could not send <a CSTA/an ACS> Universal Failure Confirmation Event (error=<error-string>) to session ID <session-ID> for invoke ID <invoke-ID> because there is not a Client Application Session (CAS) object for this session. The stream may have been closed.

  Also, the error level associated with this message has been changed from CRITICAL to WARNING.

The following issues have been resolved concerning TSAPI Service

- Previously, within the TSAPI Service, the device history in the private data of a CSTA Connection Cleared event would sometimes contain value EC_KEY_CONFERENCE instead of EC_NONE.
- Previously, licenses were not available for up to 10 minutes after a system crash, such as a power failure. Now, this service is available immediately after the system reboots.
- Previously, when using private data version 7 or later, the confirmation event for the TSAPI cstaSnapshotCallReq() service always included private data, even when there was not a device history associated with the call.
- Previously, if a TSAPI application opened a stream with private data version 5 or later and used function attSetAgentState() to format the private data accompanying a cstaSetAgentState() request, the TSAPI Service would reject the request with CSTA error VALUE OUT OF RANGE.
- Previously, if a TSAPI application attempted to add a seventh party to a conference call, the TSAPI Service would deny the request with error GENERIC SYSTEM RESOURCE

AVAILABILITY. In this scenario, the TSAPI Service now provides error CONFERENCE MEMBER LIMIT EXCEEDED.

- Previously, when a TSAPI application used the cstaMakePredictiveCall() service, in some scenarios the device ID type for the called device would change from DYNAMIC_ID (a dynamic device ID) to STATIC_ID (a static device ID).

- Previously, the device ID type for the distributingDevice field in TSAPI private data was always reported as EXPLICIT_PRIVATE_LOCAL_NUMBER. The TSAPI Service has been updated to set the device ID type for this field using numbering plan and address type information provided by Avaya Communication Manager.

The following issues have been resolved concerning OAM

- AES OAM has many HTML input fields, and some of them had cross-site-scripting (XSS) vulnerability. These XSS vulnerabilities were fixed by adding input data validation logic.

- If a user enters a switch name more than 14 characters, then OAM will verify if the first 14 characters is unique.

- Previously AE Services allowed the user to set "Default Global PanLimits" to 0. Now, if the "Existing list" is empty, and users try to set "Default Global PanLimits" to 0, an error message will be displayed.

- When CTI links are created, if duplicated data is entered, the error message will specify on what data was duplicated. For example: previously, the error message is "Duplicate data already exists"; now the message states "Duplicate data already exists: The combo of Switchname <switch name> and CTI Link Num <number> already in USE."

- Another status column was added on to the OAM Welcome Page to display the state of each service.

The following issues have been resolved concerning Certificates

- An enhancement was added to handle the certificate extension Subject Alternative Name criticality=true option. This was because the JDK version installed on AES does not support the option when it is set to true.

The following issues have been resolved concerning the SAMP

- Previously, on a fresh install of the AE Services 4.2 Bundled Server, the SAMP service failed to deploy correctly resulting in no execute privileges on the following two directories:

  /etc/opt/ecs
  /etc/opt/ecs/rmb

  This issue has been corrected in the AE Services 4.2.1 release.

DOCUMENTATION UPDATES AND CORRECTIONS

Avaya MultiVantage® Application Enablement Services
Installation and Upgrade Guide for a Bundled Server Release 4.2

Section - Setting up the AE Server for remote access

On page 35 of 100 states:

"2. Make a note of this IP address. You will need to use it when you edit the /etc/hosts file and the /etc/ppp/options.ttyUSB0 file on the AE Server."

Editing the /etc/ppp/options.ttyUSB0 or /etc/ppp/options.ttyACM0 file, depending on the type of modem:

The section should read:

"2. Make a note of this IP address. You will need to use it when you edit the appropriate files on the AE Server for the specific modem used."

Avaya MultiVantage® Application Enablement Services
Administration and Maintenance Guide

Chapter 1: Administering Communication Manager for AE Services

Enabling Processor Ethernet Support

On the S8300 and S8400 media servers, Processor Ethernet support is enabled by default.
On the S85xx media server, Processor Ethernet support is not enabled by default.

To enable AE Services Processor Ethernet support on the S85xx, first enable the Processor Ethernet feature on the System Parameters Customer Options form, then administer the processor interface with the add ip-interface procr command.

Follow this procedure:
1. Type **display system-parameters customer-options**.
   - Verify Processor Ethernet is enabled.
   - Processor Ethernet must be enabled before proceeding to the next task.
     Note: Processor Ethernet support on the S85xx requires CM 3.1 or later.

2. Type **add ip-interface procr**

Important: Processor Ethernet support on the S85xx limits the CTI Message rate to 240 messages per second duplex.

Documentation Correction:
Page 34

Enabling AE Services

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services.

<4.2.1 Release Notes> Step 2 in the current documentation needs to be changed to the following:

2. Complete Page 1 of the IP SERVICES form, as follows:
● In the Service Type field, type **AESVCS**.
● In the Local Node field type the appropriate entry, as follows:
- On an S8300, S8400, S85xx*; type **procr**.

Note: *Make sure Processor Ethernet support has been enabled on the S85xx.

- On all other systems, type *<**nodename**>* (where *<**nodename**>* is the name of the CLAN board you will use on an S8400, S85xx, S87xx, or DEFINITY Server Csi. You can locate node names by typing **display node-names ip** and checking the Local Node field on the IP NODE NAMES form.
● In the Local Port field, accept the default (**8765**).

Note: If you are adding more than one CLAN for AE Services, repeat Step 2 for each CLAN you add.

New Configuration Changes for Bridge Appearance Alert for Microsoft Office Live Communications

OAM Admin Guide for Bridged Appearance Alert Configuration

When you are administering AE Services for usage with Microsoft Office Live Communications Server you can use the Bridged Alert Configuration (Bridged Alert Config) feature in AE Services OAM to control the number of bridged appearances that appear on an assistant's desktop -- Microsoft Office Communicator will display a pop-up conversation window whenever a call appears for a bridged appearance.

By default, bridged call appearances generate an alert. This means that an assistant whose phone is administered with a bridged call appearance will receive an alert pop-up whenever an executive receives a call. The idea of managing or restricting bridged alerts comes into play when an assistant is administered with multiple bridged call appearances. In effect you are setting up a filter, based on the mapping of an assistant to an executive, or group of executives using the AES OAM web interface.

Access the Bridged Appearance Alert Configuration link

1. Login to OAM as a user with System Administrator privileges.
2. Select CTI OAM Administration→Administration→Bridged Alert Config
3. OAM shall display "Bridged Appearance Alert Configuration" page.

Block Bridged Appearance Alerts

The checkbox labeled "Block Bridged Appearance Alerts" is unchecked (default setting).

Calls to bridged appearances on any assistant station will cause an Office Communicator incoming call alert window for the bridged extension to be displayed. The assistants in the "Rule Exceptions" list will not receive a call alert window.

a. To add an assistant to the "Rule Exceptions" list, see the section **Add Bridged Appearance Rule Exception**.

b. To edit an assistant in the "Rule Exceptions" list, see the section **Edit a Bridged Appearance Rule Exception**.

Unblock Bridged Appearance Alerts

The checkbox labeled "Block Bridged Appearance Alerts" is checked

Calls to bridged appearances on any assistant station will NOT because an Office Communicator incoming call alert window for the bridged extension to be displayed. The assistants in the "Rule Exceptions" list will receive a call alert window.

- To add an assistant to the "Rule Exceptions" list, see the section **Add Bridged Appearance Rule Exception**.
- To edit an assistant in the "Rule Exceptions" list, see the section **Edit a Bridged Appearance Rule Exception**.

Add Bridged Appearance Rule Exception

1. Click the Add button
2. Add Bridged Appearance Rule Exceptions page will be loaded.
3. In the "Assistant Login ID" field, enter the login id of the assistant.
4. In the "Executive Login ID" field, enter the login id of the executive.

5. If the assistant is associated to multiple executives, click the “Add Executive” button, another text box will be displayed for entering the other executive login IDs.
6. Click the “Apply Change” button
7. On the confirmation page verify each TelUri and User Name is correct.
8. If not correct, click the “Cancel” button to edit the entered data, otherwise click “Apply”
9. The Bridged Alert Configuration page will be reloaded with the new data.

Edit a Bridged Appearance Rule Exception

1. Select the rule exception that you want to modify
2. Click the Edit button
3. Edit Bridged Appearance Rule Exceptions page will be loaded
4. Modify the Executive Login ID fields, or click the “Add Executive” button to add additional executives.
5. Click the “Apply Change” button
6. On the confirmation page verify each TelUri and User Name is correct.
7. If not correct, click the “Cancel” button to edit the entered data, otherwise click “Apply”
8. The Bridged Alert Configuration page will be reloaded with the new data.

Delete a Bridged Appearance Rule Exception

1. Select the rule exception that you want to delete
2. Click the Delete button
3. The Confirmation page is loaded
4. If you really want to delete this rule, click the “Apply” button, otherwise click the “Cancel” button

View the details of a Bridged Appearance Rule Exception

1. Select the rule that you want to view
2. The corresponding detail page will be displayed, which includes the Login ID, User Name and TelUri of an Assistant and the associated Executives.

Synchronize the data stored by AES with LDAP

1. Click the “Synchronize” button.
2. The Confirmation page will be loaded.
3. If you want to continue the synchronization, click the “Apply” button. This function will synchronize the rule exception data in the AES OAM database with the customers LDAP data. Once the process completes, if an assistant does not exist in LDAP anymore, the rule exception for the assistant will be removed; In addition any associated executives will be removed. If an executive does not exist anymore, the executive will be removed from the corresponding rule exception list.

TEG (Terminating Extension Group)

Currently, TEG is treated the same as a bridged appearance call.

1. Assign the group number to a MOC user.
   - Group number is the extension of the executive.
   - Member number is the extension of the assistant.
2. Repeat the steps in the following sections:
   - **Add Bridged Appearance Rule Exception**
   - **Edit a Bridged Appearance Rule Exception**