Product Support Notice

PSN #	PSN020534u				
Original publication date: 01-Aug-21. This is Issue #16, published date: 11-Aug-22.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN020534u - Avaya Aura® Application Enablement Services (AES) ACTION REQUIRED				

Products affected

Avaya Aura® Application Enablement Services (AES), All releases

Problem description

August 11, 2022 Update – Additional instructions for hotfix on AES 4.x – requires update to AES 4.2.4.

August 2, 2022 Update – Additional instructions when applying hotfix on AES 5.x.

April 8, 2022 Update – A new script is available to check if an ASL application is connected to AES. "check_asl_v2" will not apply the hotfix, but will allow for the identification of an ASL application. This supersedes the use of the "-u" option in the ASL hotfix. The "-u" option should no longer be used.

March 1, 2022 Update – there was an issue with the hotfix uploaded to PLDS that required reposting the hotfix.
If you downloaded hotfix AES00000903, please ensure that the md5sum matches the following. If it does not, please download the hotfix again.

md5sum /tmp/AES_28516_Hotfix.bin
5d1a8925df0f6f5afbd3dfc352e7a625 AES_28516_Hotfix.bin

If the hotfix was applied and the md5sum does not match the above, you will need to remove the hotfix (instructions in the Patch Notes section of this PSN), download the hotfix from PLDS again, verify the md5sum and install the newly downloaded hotfix.

ACTION REQUIRED

Application Specific Licensing (ASL), also known as "Named Licensing," allows approved Avaya and specific third-party applications to acquire special licensing privileges that are not available to standard applications. These licensing privileges are used by Avaya to ensure compliance with the terms and conditions of our commercial offers.

ASL uses an Avaya verification mechanism to connect to the approved applications. The list of approved applications includes, but is not limited to those listed in the table below. CTI applications require an update only when compatibility with AES R10.1 or later releases is needed. As application specific updates are made available, a link to the corresponding application specific PSN will be added in the table below.

• Contact Center Express / Elite Multichannel • Customer Interaction Express • Avaya Aura® Presence Services • Proactive Contact *PSN006065u* • Voice Portal with Dialog Designer • Avaya Aura® Experience Portal • Avaya Workforce Engagement/Avaya Aura® Workforce Optimization *PSN006074u* • Avaya Workforce Engagement Select *PSN006079u* • Avaya one-X® Attendant • CallBack Assist • StationLink • StationLink Web	• StationLink Toolbar • Agent MAP • CallRouting • CC-One Portal • Avaya Navigator • CM Adaptor Agent States • Oceana *PSN006072u; PSN006076u* • Workspaces *PSN006072u; PSN006076u* • Elite Call Control (ECC) *PSN006072u; PSN006076u* • SFDC Connector / Workspaces for SalesForce • CRM Connector	• Open CTI Adapter / CTI Engine • Avaya custom widgets • Avaya Aura® WorkForce Optimization Select • Officelinx / Avaya Messaging • Avaya Cloud Application Link • CRM Routing Adapter • Avaya Conversational Intelligence • SAP Connector • Siebel CTI Driver • Oracle Service Cloud Connector • Harmony Workforce Optimization

The current ASL verification mechanism implemented by Avaya will expire on **August 23, 2022.**

For existing applications, once the expiration date is reached, if the AES is restarted or the link between AES and the CTI application is restarted, the connection will NOT establish, and *the supported applications will no longer function*.

All customers using ASL *MUST* take action as described below.

Descriptions in related Avaya documentation such as "AES Update Script" can be considered all-inclusive for the delivery options that are detailed in this PSN.

Resolution

ACTION REQUIRED 10.1.x and later releases

New ASL updates are included in AES 10.1.0 and later with an expiration date of July 15, 2033.
AES release 10.1 or later releases will work with CTI applications that have not been so updated until the first time AES is restarted, or the link between AES and the CTI application is restarted, on or after August 23, 2022.
As CTI applications are updated, customers should plan to implement the updated versions prior to August 23, 2022 to ensure the CTI application will continue to function after August 23, 2022.

ACTION REQUIRED for Release 8.1.3.4 (GA Feb 22, 2022)

Once AES is updated to 8.1.3.4 or later Service Pack, changes are not required to the CTI applications. (CTI applications require an update only when compatibility with AES R10.1 or later releases is needed.)

ACTION REQUIRED for Release 8.1.3.3

Avaya is introducing AES 8.1.3.3 Super Patch 2 (8.1.3.3.2)
Reference *PSN020562u- Avaya Aura® Application Enablement (AE) Services 8.1.3.x Super Patches*
Once AES is updated to 8.1.3.3.2, changes are not required to the CTI applications. (CTI applications require an update only when compatibility with AES R10.1 or later releases is needed.)

ACTION REQUIRED for Release 4.x through 8.1.3.2

NOTE: AES 4.x requires update to AES 4.2.4
Step 1: Detection of ASL applications using *check_asl_v2.bin* script.
Step 2: Application of hotfix *AES_28516_Hotfix.bin*.

Avaya has released a new script (*check_asl_v2*) that will assist in determining if an ASL application is connected to AES. This script is separate and independent of the software update hotfix. This script is not service impacting and can be run at any time as it does not restart any services.

Release	Script to check for presence of ASL connections (live or previous) to AES	GA Date	Notes
4.x – 8.1.3.2 ***NOTE: AES 4.x requires update to AES 4.2.4***	check_asl_v2.bin PLDS ID: *AES00000906*	Apr 8, 2022	Follow instructions in the Patch Notes section of this PSN. Requires root credentials

Critical Note: This non-intrusive script (*check_asl_v2*) will in most cases detect the presence of an ASL application and indicate whether you need to apply the Hotfix for this issue. However, in certain instances the script will not detect the presence of an ASL Application. Therefore, if the presence of an ASL application is not detected but there is a chance you may have an ASL application connected to AES, as a precaution you should install the AES_28516_Hotfix with the '-f' option to ensure there are no risks to your environment due to this issue. Avaya has not identified any issues with application of the hotfix on systems that do not utilize ASL. Therefore, if uncertain, application of the hotfix is recommended.

For these releases, Avaya is introducing an AES-only software update hotfix. Once AES is updated, changes are not required to the CTI applications. (CTI applications require an update only when compatibility with AES R10.1 or later releases is needed.)

Critical Note: The software update hotfix AES_28516_Hotfix.bin does not persist across any additional hotfix, Super Patch or upgrade. It will need to be re-applied after every subsequent update/upgrade.

Release Vehicle of the ASL Fix

These updates are now available and should be applied at the earliest opportunity, well in advance of the August 23, 2022 expiration.

Release	Release Vehicle of the ASL Fix	GA Date	Notes
4.x – 8.1.3.2 ***NOTES:*** **** AES 4.x requires update to 4.2.4*** ****Special steps for 5.x as noted in Patch Notes section of this PSN.***	AES_28516_Hotfix.bin PLDS ID: *AES00000903*	Feb 28, 2022	Follow instructions in the Patch Notes section of this PSN. Requires root credentials. Requires update to AES 4.2.4 before applying hotfix. Special steps for AES 5.x.
8.1.3.3	8.1.3.3.2 Super Patch *aesvcs-8.1.3.3.2-superpatch.bin* PLDS ID:*AES00000901*	Feb 4, 2022	Reference *PSN020562u- Avaya Aura® Application Enablement (AE) Services 8.1.3.x Super Patches* Utilize SDM to install the Super Patch. If installing via CLI method, root credentials are required.
8.1.3.4	Included in AES 8.1.3.4 Service Pack	Feb 22, 2022	Reference *PCN2102S* Utilize SDM to install the Service Pack. If installing via CLI method, root credentials are required.

Workaround or alternative remediation

N/A

Remarks

Issues 1-5 Avaya Internal Communication Only
Issue 6 – February 04, 2022: Solution available for 8.1.3.3.
Issue 7 – February 14, 2022: Tentative Target 8.1.3.4 GA date moved to Feb 21.
Issue 8 – February 28, 2022: Updated GA date for 8.1.3.4; updated hotfix installation instructions; hotfix PLDS ID available.
Issue 9 – March 1, 2022: hotfix replaced on PLDS – please verify md5sum to ensure you have correct version.
Issue 10 – March 4, 2022: Updated for High Availability.
Issue 11 – March 7, 2022: Additional clarification for High Availability.
Issue 12 – April 8, 2022: Updated FAQ link, new *check_ASL_v2.bin* script available, deprecate "-u" option on hotfix.
Issue 13 – April 12, 2022: Updated to clarify if uncertain if ASL is utilized, application of hotfix recommended.
Issue 14—July 11, 2022: Updated to add additional application PSN links.
Issue 15 – August 2, 2022: Updated with special instructions for AES 5.x.
Issue 16 – August 11, 2022: Updated with special instructions for AES 4.x. Updated to add additional application PSN links.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Backup AE Services server data before applying any updates.

1. Log into the AE Services Management Console using a browser.
2. From the main menu, select **Maintenance > Server Data > Backup**.
   AE Services backs up the database, and displays "`The backup file can be downloaded from Here`" on the **Database Backup** screen,
3. Click the "**Here**" link.
   A file download dialog box is displayed, from where you can open or save the backup file *serverName_SoftwareVersion*_aesvcsdb*ddmmyyyy*.tar.gz. Where, ddmmyyyy is the date stamp).

4. Click **Save**, and download the backup file to a location from where you can gain access after the system upgrade. For example, save the file to your local computer or another computer used for storing backups.

Download

AES 8.1.3.4

Reference PCN2102S

Release 8.1.3.3

Download *aesvcs-8.1.3.3.2-superpatch.bin;* PLDS ID:*AES00000901*
Reference *PSN020562u- Avaya Aura® Application Enablement (AE) Services 8.1.3.x Super Patches*

Release 4.x – 8.1.3.2

NOTE: 4.x requires update to 4.2.4 prior to applying hotfix

Download *check_asl_v2.bin;* PLDS ID: *AES00000906*
Reference *Patch install instructions* in this PSN.

Download AES_28516_Hotfix.bin; PLDS ID: *AES00000903*
Reference *Patch install instructions* in this PSN.

Release 5.x ONLY may require download of the *binutils* rpm. The following link is the only supported version of *binutils* that can be used with AES 5.x.
AES 5.x - https://vault.centos.org/5.3/os/i386/CentOS/binutils-2.17.50.0.6-9.el5.i386.rpm

Patch install instructions	Service-interrupting?

AES 8.1.3.4 Yes

Reference PCN2102S. Utilize SDM to install the Service Pack. Utilize SDM to install the Service Pack. If installing via CLI method, root credentials are required.

AES 8.1.3.3

Reference *PSN020562u- Avaya Aura® Application Enablement (AE) Services 8.1.3.x Super Patches* for Super Patch install instructions. Utilize SDM to install the Super Patch. If installing via CLI method, root credentials are required.

AES 4.x – 8.1.3.2 (two steps, 1 - detection of ASL via check_asl_v2.bin script, 2 - application of hotfix)

NOTES:

- **AES 4.x requires update to AES 4.2.4 before applying hotfix.**
- **AES 5.x may require an additional step, to download and install the *binutils* rpm. Reference instructions prior to Step 2 below.**

1) Execution of the *check_asl_v2.bin* script to detect live or previous ASL connections.

Avaya recommends that the *check_asl_v2.bin* script be executed prior to applying the hotfix.
The *check_asl_v2.bin* script will not apply the hotfix, but will allow for the identification of an ASL application that is currently connected to AES or in some cases, will be able to identify that an ASL application was previously connected. This supersedes the use of the "-u" option in the ASL hotfix. The "-u" option should no longer be used.
If the "-u" option in the hotfix was previously utilized, it is recommended to run the *check_asl_v2.bin* script.

There will be some instances where identification of ASL connections via the logs is not possible if logging was not enabled or logs have rotated. Therefore, if uncertain, application of the hotfix is recommended.

1. Copy *check_asl_v2.bin* into /tmp on the AES server
2. Verify the MD5sum of the file matches *2ee773be00448692b734fba5ff185c90*
   md5sum /tmp/ check_asl_v2.bin
   2ee773be00448692b734fba5ff185c90 check_asl_v2.bin
3. Give executable permission to *check_asl_v2.bin*
   chmod +x /tmp/ check_asl_v2.bin
4. Switch to root user

5. Execute the script
   /tmp/check_asl_v2.bin

The following table provides the three possible outputs from execution of the *check_asl_v2.bin* script.

	check_asl_v2 Output	AES R4.x - R5.x	AES R6.x - R8.x
1	*One or more Application Specific Licensing (ASL) application/s are connected to this AES Server*	N/A See Row 2 below under R4.x-R5.x	TSAPI and/or DMCC ASL Applications are currently connected to AES.
2	*System logs indicate presence of previous Application Specific Licensing (ASL) application(s) connections to this AES Server. However, no Application Specific Licensing (ASL) application/s are currently connected to this AES Server.*	TSAPI and/or DMCC ASL Applications are currently connected to AES. ***OR*** TSAPI and/or DMCC ASL Applications were connected to this AES at an earlier point in time.	TSAPI and/or DMCC ASL Applications were connected to this AES at an earlier point in time.
3	*No Application Specific Licensing (ASL) configurations were identified on this AES server. Please note that the script may not detect all ASL configurations. For complete technical details, please refer to PSN020534.*	No TSAPI or DMCC ASL applications are currently connected or were connected to this AES at an earlier point in time. ***OR*** TSAPI and/or DMCC logging has been disabled on the system thus preventing the detection of ASL Application, both active and non-active, connections.	No TSAPI or DMCC ASL applications are currently connected or were connected to this AES at an earlier point in time. ***OR*** TSAPI and/or DMCC logging has been disabled on the system thus preventing the detection of ASL Application, both active and non-active, connections.

STOP: If AES 5.x, execute the following steps:

a. Check to see if the *binutils* rpm is installed on AES 5.x by executing the following command:
   rpm -qi binutils
   If there is no output, it is not installed.
b. If the *binutils* rpm is already installed, proceed to Step 2 below as no further action is required.
c. If the *binutils* rpm is NOT installed, download the rpm from the following link and copy into the /tmp directory on AES. Only this specific version of the rpm can be used.
   https://vault.centos.org/5.3/os/i386/CentOS/binutils-2.17.50.0.6-9.el5.i386.rpm
d. Install the *binutils* rpm using the following command:
   rpm -ivh binutils.rpm*
e. Check to ensure the *binutils* rpm was installed successfully, utilizing the same command as in step a.
   rpm -qi binutils
f. Proceed to Step 2 below to install the hotfix.

2) Application of the hotfix – ALWAYS utilize the "-f" option

- The hotfix must be installed by root user.
- The AES DMCC/CMAPI and TSAPI services will be automatically restarted after application of the hotfix.
- **Best practice is to install the hotfix during a maintenance window.**
- For AES 4.2.4 only, all CTI traffic will be lost during the installation of the hotfix. On AES 5.x-8.1.3.2, application of the hotfix will not interrupt CVLAN or DLG CTI traffic.
- It will take ~ 5 minutes for the hotfix to install on AES 4.2.4 and ~ 2 minutes to install on AES 5.x-8.1.3.2. Once the prompt is back, the services will be restarting. It may take up to 5 minutes for the services to be fully restarted
- Instructions for High Availability (HA)– this includes the different types of HA based on release: Geo Redundant High Availability (GRHA), Fast Reboot High Availability (FRHA), Machine Preserving High Availability (MPHA).
  - HA does not need to be stopped regardless of the type of HA (GRHA, FRHA, MPHA).

    - GRHA – the hotfix must be applied on both Primary and Standby servers.
        - Do not install the hotfix on Standby if the hotfix installation was unsuccessful on Primary.
    - FRHA and MPHA – memory replication ensures hotfix will be replicated to standby once applied on primary. Wait 5 minutes to ensure replication is complete.
- **NOTE**: Avaya has not identified any issues with application of the hotfix on systems that do not utilize ASL. Therefore, if uncertain, application of the hotfix is recommended.

Critical Note: The software update does not persist across any additional hotfix, Super Patch or upgrade. It will need to be re-applied after every subsequent update/upgrade.

AES_28516_Hotfix.bin is applicable to all AES versions 4.2.4 through 8.1.3.2. It should not be applied on 8.1.3.3 or later. If it is accidentally applied on a later version, it must be removed.

Instructions for hotfix:

1. Verify the status of the "aesvcs" service is in Active mode. From the AES CLI, execute the following:
   service aesvcs status
    - If the status is not active, Avaya recommends investigation as to why "aescvs" is not running before proceeding with hotfix installation.
    - If hotfix installation proceeds when "aesvcs" is not active, the output from the installation of the hotfix will differ on 5.x-8.1.3.2.
    - If "aesvcs" is not running, DMCC and TSAPI Services messages will be replaced with mvap service messages.
2. Copy AES_28516_Hotfix.bin into /tmp on the AES server
3. Verify the MD5sum of the file matches *5d1a8925df0f6f5afbd3dfc352e7a625*
   md5sum /tmp/AES_28516_Hotfix.bin
   5d1a8925df0f6f5afbd3dfc352e7a625 AES_28516_Hotfix.bin
4. Give executable permission to AES_28516_Hotfix.bin
   chmod +x /tmp/AES_28516_Hotfix.bin
5. Switch to root user
6. Always utilize the "-f" option when applying the hotfix.
7. It will take ~ 2 minutes for the hotfix to install. Once the prompt is back, the services will be restarting. It may take up to 5 minutes for the services to be fully restarted.
8. Example output for the different scenarios. Note that there will be slightly different output of the hotfix installation for AES 4.2.4

Installation of the hotfix. Always utilize the "-f" option.

Release 4.2.4:

```
[root@AESserver]# /tmp/AES_28516_Hotfix.bin -f
        Patch Name: AES_28516_Hotfix

        ********************************* WARNING **********************************
        Hotfix Installation will be service impacting.
        Do you want to continue? y or n
        ****************************************************************************
        > y

        Entering pre-install function...
        Stopping mvap Service
        Taking Backup of original files

        ***** Installing hotfix *****

        Copying files to their respective location on AES
        Entering post-install function...
        Installation of hotfix is successful
        Starting mvap Service
```

```
        The AES_28516_Hotfix hotfix installation operation successfully completed.
```

Release 5.x – 8.1.3.2

```
[root@AESserver]# /tmp/AES_28516_Hotfix.bin -f
        Patch Name: AES_28516_Hotfix

        ********************************* WARNING **********************************
        Hotfix Installation will be service impacting.
        Do you want to continue? y or n
        ****************************************************************************
        > y



        Entering pre-install function...
        Stopping DMCC and TSAPI Services
        Taking Backup of original files

        ***** Installing hotfix *****

        Copying files to their respective location on AES
        Entering post-install function...
        Installation of hotfix is successful
        Starting DMCC and TSAPI Services
        The AES_28516_Hotfix hotfix installation operation successfully completed.
```

NOTE: If application of the hotfix on AES 5.x results in the following error, ensure that the *binutils* rpm is installed as noted in the instructions above.

```
root@AESserver]# /tmp/AES_28516_Hotfix.bin -f
        Patch Name: AES_28516_Hotfix

        ********************************* WARNING **********************************
        Hotfix Installation will be service impacting.
        Do you want to continue? y or n
        ****************************************************************************
        > y

        Entering pre-install function...
        Stopping DMCC and TSAPI Services
        Taking Backup of original files

        ***** Installing hotfix *****

        Copying files to their respective location on AES
        TSAPI hotfix installation is not successful. Error code= 5
        Uninstalling the hotfix
        Backup Files present. Continuing Uninstallation
        Uninstallation of hotfix is successful
        Starting DMCC and TSAPI Services
        Hotfix ./AES_28516_Hotfix hotfix installation operation failed.
```

Verification

Ensure that the services have fully restarted.

Release	Service Status Commands
AES 4.2.4	[cust@aes4swonly ~]$ mvap.sh status **CmapiService** CmapiService : **Running** [cust@aes4swonly ~]$ mvap.sh status **TsapiService** TsapiService : **Running**
AES 5.x/6.x/7.x/8.x	[cust@aesasl524 ~]$ mvap.sh status **DmccService**

	DmccService : **ONLINE** [cust@aesasl524 ~]$ mvap.sh status **TsapiService** TsapiService : **ONLINE**

If status is initializing, wait a few minutes and recheck to ensure ONLINE/Running.

Execute the swversion command and ensure the AES_28516_Hotfix is displayed in the "*Patch Numbers Installed in this system are*" field.
The following is an example for 4.2.4:

```
[sroot@aesasl524 cust]# swversion
********************************************************************************
Avaya Connector Server
********************************************************************************
Version: r4-2-4-35-0
Server Type: unknown
Offer Type: bundled

********************************************************************************
Operating System Version
Linux 2.6.9-89.0.26.ELsmp
************* Patch Numbers Installed in this system are  *************
AES_28516_Hotfix
********************************************************************************
Use "swversion [-a | --all]" to get a complete list of AE Services RPMS and Patches/Updates
```

The following is an example for AES 8.1.3.0

```
[root@AESserver]# swversion
********************************************************************
Application Enablement Services
********************************************************************
Version: 8.1.3.0.0.25-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
RTS Version:AES8.1.3.0.0.25-0

********************************************************************
Operating System Version: Linux 3.10.0-1062.12.1.el7.x86_64

**************Patch Numbers Installed in this system are ***********
FP8.1.3.0.0.25 (AES 8.1.3)
AES_28516_Hotfix
********************************************************************
Use "swversion [-a | --all]" to get a complete list of AE Services RPMS and Patches/Updates
```

The following is an example for AES 8.1.3.2

```
[root@AESserver]# swversion
********************************************************************************
Application Enablement Services
********************************************************************************
Version: 8.1.3.2.0.4-0
Server Type: OTHER
Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
RTS Version:AES-8.1.3.2.0.4-0

********************************************************************************
Operating System Version: Linux 3.10.0-1062.12.1.el7.x86_64

************* Patch Numbers Installed in this system are  *************
FP8.1.3.2.0.4 (AES 8.1.3)
```

```
AES_28516_Hotfix
**************************************************************************
Use "swversion [-a | --all | -s]" to get a complete list of AE Services RPMS and Patches/Updates
```

Failure

If installation of the hotfix on AES 5.x results in “Error code= 5” and fails, ensure that the *binutils* RPM is installed as described in the Patch Notes section of this PSN. Contact Avaya Services for all other failures.

Installation of the hotfix will fail on AES <4.2.4 and may result in “Error code= 6”. For AES 4.x, the hotfix can only be installed on AES 4.2.4.

Patch uninstall instructions

AES 8.1.3.4

Reference PCN2102S.

AES 8.1.3.3.2: Reference *PSN020562u- Avaya Aura® Application Enablement (AE) Services 8.1.3.x Super Patches* for Super Patch uninstall instructions.

AES 4.2.4 – 8.1.3.2

Execute */tmp/AES_28516_Hotfix.bin -e* as a root user.

Example output for AES 4.2.4

```
[root@aes4swonly cust]# ./AES_28516_Hotfix.bin -e
        Patch Name: AES_28516_Hotfix
        Uninstalling the hotfix
        Backup Files Present. Continuing Uninstallation
        Stopping mvap Service
        Uninstallation of hotfix is successful
        Starting mvap Service
        The AES_28516_Hotfix hotfix uninstallation operation successfully completed.
```

Example output for AES 5.x – 8.1.3.2

```
[root@AESserver]# /tmp/AES_28516_Hotfix.bin -e
        Patch Name: AES_28516_Hotfix
        Uninstalling the hotfix
        Backup Files Present. Continuing Uninstallation
        Stopping DMCC and TSAPI Services
        Uninstallation of hotfix is successful
        Starting DMCC and TSAPI Services
        The AES_28516_Hotfix hotfix uninstallation operation successfully completed.
```

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

N/A

Avaya Security Vulnerability Classification

N/A

Mitigation

N/A

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms..

INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.