



Product Support Notice

© 2015 Avaya Inc. All Rights Reserved.

PSN # PSN027020u

Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 21-May-15. This is Issue #6, published date: 28-Feb-18.

Severity/risk level Medium Urgency Optional

Name of problem PSN027020u – HP DL360P G8 Firmware Update

Products affected

Common Server R2 (HP DL360P G8)
Avaya Aura® System Platform 6.3.x, 6.4.x
Avaya Aura® Appliance Virtualization Platform (AVP) 7.x
Avaya Proactive Contact 5.1.1 & higher
Avaya Aura® Experience Portal 7.x

Problem description

HP has suggested firmware updates to resolve an issue with older firmware versions and HP Integrated Lights Out (iLO). The firmware that shipped with the G8 servers initially is version 2.2 which includes iLO 1.22. HP recommends going with later versions of their firmware as they have addressed some stability issues since the iLO 1.22 release.

The updates to the firmware include:

1. Fix for Cipher Suite 0 security issue identified in CVE-2013-4805.
2. P410i, P420i RAID controller fixes added: HDD error cases, battery and Super Cap reporting problems showing erroneous low charge corrected
3. BIOS updates: Critical Intel Micro code updates required
4. Broadcom NIC devices - fixes for PCIe link training

Avaya Common Server Team has provided the HP DL360P G8 server firmware version 4 to the Avaya Aura System Platform, Appliance Virtualization Platform (AVP), and application CPE/T4 teams.

Session Manager, which does not utilize System Platform, has a separate PSN that addresses firmware upgrades specifically for Session Manager running on an HP DL360P G8.

Avaya Aura® Session Manager (see [PSN004481u](#))

NOTE: This firmware is customer installable.

You should always utilize the certified, bundled release. Do NOT upgrade individual components. HP releases bundles called SPPs (Service Pack for ProLiant). This ensures that the components have been tested together for dependencies. Avaya then creates a tailored HP SPP firmware update tool for our Common Server Configurations that goes through additional testing.

Resolution

The following procedure describes how to run the firmware update tool on an Avaya HP DL360P G8. When the update tool is run it will indicate firmware versions currently installed on the server. After executing the procedures, the following components will be updated to the listed firmware versions:

The DL360G8 Firmware update (v4.0) disc contains:

Device Information	Firmware package release	Firmware Version
iLO 4	CP025108.scexe	V2.03
Power Management Control	CP021615.scexe	V3.3
Power Management Control	CP021012.scexe	V1.6
P71 BIOS (DL360PG8)	CP024481.scexe	2014.08.02

P72 BIOS (DL380PG8)	CP024431.scexe	2014.08.02
P420i SMART ARRAY Cntrl (RAID Controller)	CP023886.scexe	V6.00
HP NC Series Broadcom Firmware (331FLR and 332T)	CP023977.scexe	2.13.5
HP NC Series Broadcom Firmware (331FLR and 332T)	CP0131168.scexe	2.2.7
HDD Firmware Models: EG0146FAWHU, EG0300FAWHV, DG0146FAMWL, DG0300FAMWN	CP020194.scexe	HPDF(C)
HDD Firmware Models: EH0146FCBVB and EH0300FCBVC Drives	CP023185.scexe	HPD4
HDD Firmware Models: EH0146FBQDC and EH0300FBQDD Drives	CP023184.scexe	HPD3
HDD Firmware Models: EH0072FARWC and EH0146FARWD Drives	CP023183.scexe	HPDD
HDD Firmware Models: EH0072FARUA and EH0146FARUB Drives	CP023182.scexe	HPD9
HDD Firmware Models: EG0300FBVFL, EG0450FBVFM, EG0600FBVFP, and EG0900FBVFQ Drives	CP021542.scexe	HPD9
HDD Firmware Models: EG0300FBVFL, EG0450FBVFM, EG0600FBVFP, and EG0900FBVFQ Drives	CP023179.scexe	HPDC
HDD Firmware Models: EG0300FCVBF, EG0450FCVBH, EG0600FCVBK, and EG0900FCVBL Drives	CP023180.scexe	HPD5
HDD Firmware drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP017743.scexe	HPD7
HDD Firmware drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP015559.scexe	HPD6
HDD Firmware Models: EG0300FBLSE, EG0450FBLSF, EG0600FBLSH, and EG0900FBLSK Drives	CP023178.scexe	HPD7
HDD Firmware Drives Models: EG0300FBDBR, EG0450FBDBT and EG0600FBDBU	CP023176.scexe	HPDA
HDD Firmware Drives Models: EF0300FARMU, EF0450FARMV, and EF0600FARNA	CP023174.scexe	HPD6
HDD Firmware Models: EF0300FATFD, EF0450FATFE, and EF0600FATFF Drives	CP023175.scexe	HPDB
HDD Firmware Models: DH0072FAQRD, DH0146FAQRE, EH0146FAWJB, and EH0072FAWJA Drives	CP023173.scexe	HPDJ
HDD Firmware Models: DG0146FARVU, DG0300FARVV, DG0146BAMYQ, DG0300BAMYR, EG0146FAWJC, and EG0300FAWJD Drives	CP023172.scexe	HPDG
HDD Firmware Drives Models: EG0300FBDSP, EG0450FBDSQ, and EG0600FBDSR	CP023177.scexe	HPD6

1. HDD firmware is included in update disc to cover all possible HDD models that may have shipped in a DL360G8 server. Server may not require any and will not require all HDD firmware packages on this disc.
2. Prerequisite firmware is included on this update disc in case older server firmware requires an intermediate update before installing latest release. If a firmware update requires a prerequisite firmware release that is not on this update disc notify your AVAYA contact and report what update package is needed.

Acquiring Update Tool

Download the file, **DL360PG8fwupdate_v4.0.iso** via PLDS download ID CMCS0000009 and burn a **bootable** DVD from it.

Shut down the server according to Application Procedures

Please be aware that if the customer is on System Platform 6.3.4.08007.0, this should not be done until they upgrade to 6.3.4.08011.0 per PSN027004u.

It is always best practice to perform a complete backup of the system before any firmware or hardware maintenance.

There are two ways to gracefully shutdown a System Platform server.

1) Login to the CDOM Webconsole.

Navigate to Server Management→Server Reboot/Shutdown.

Select Shutdown Server.

You will be prompted to acknowledge the following message by selecting “OK”

This will shutdown all virtual machines and the server will be powered down. Are you really sure?

Note that the server will shutdown but the Webconsole will not provide an update as the system will have shutdown.

If the server is running System Platform 6.3.6, the server will halt, but not shut down. To completely shut down the server after executing Shutdown Server via the webconsole, ping dom0 until it does not respond and then hold the power button in for 5 sec.

2) An alternative to shutting down the server is to login to domain-0, su to root and execute “halt”.

You can confirm the server is shutdown by pinging the IP address of domain-0.

There should be no reply.

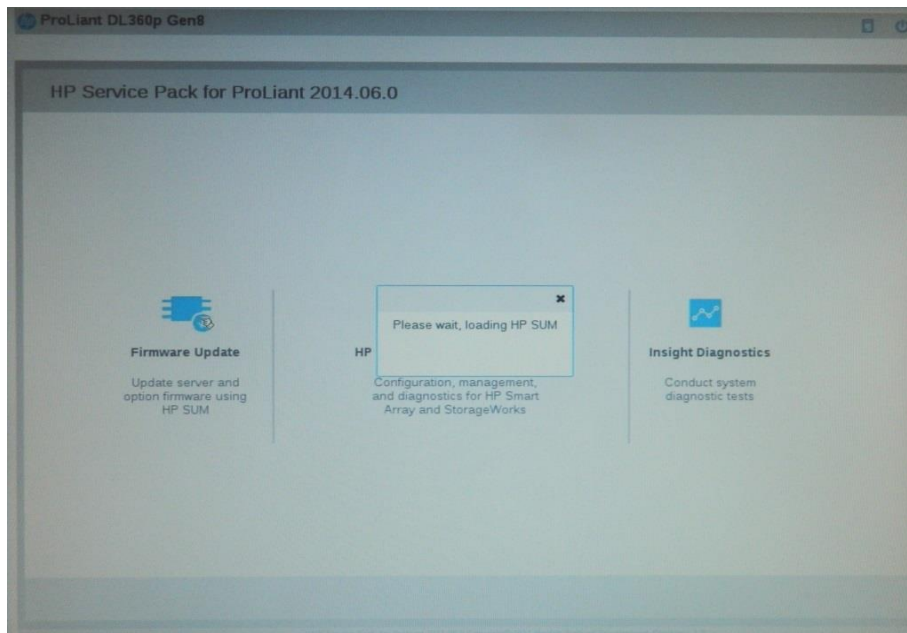
If this is an AVP server, shutdown as you normally would by performing a host shutdown via the Solution Deployment Manager.

Firmware Update Procedures

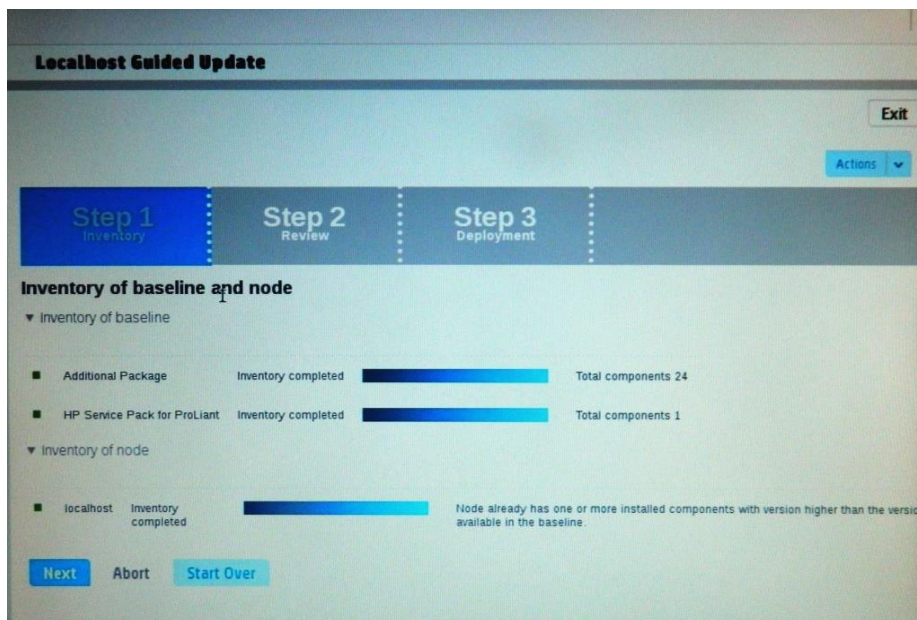
1. A Monitor, USB keyboard and mouse will be required to run the update tool.
2. Insert the firmware update disc at server power up. Server will boot from disc.
3. System will boot and load update Utility



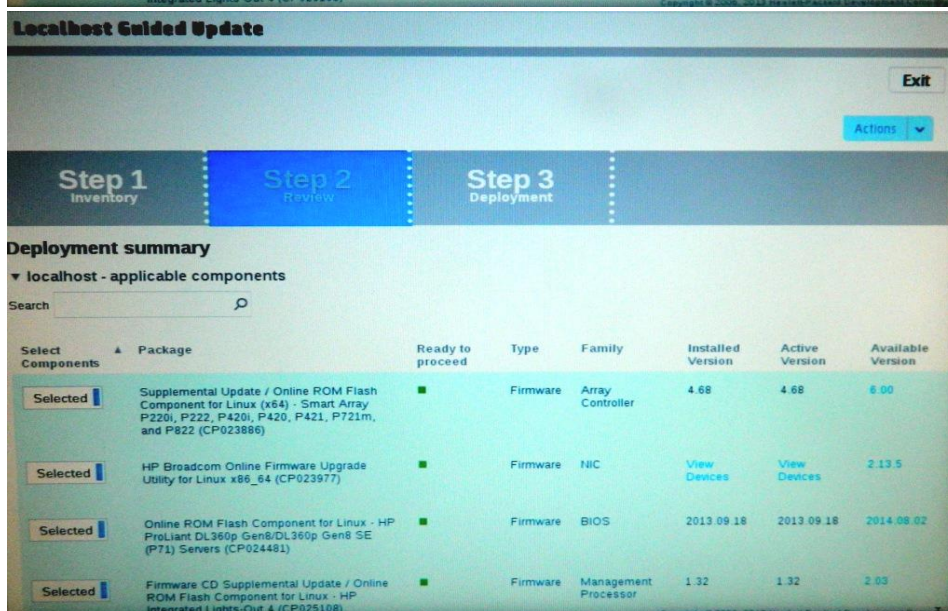
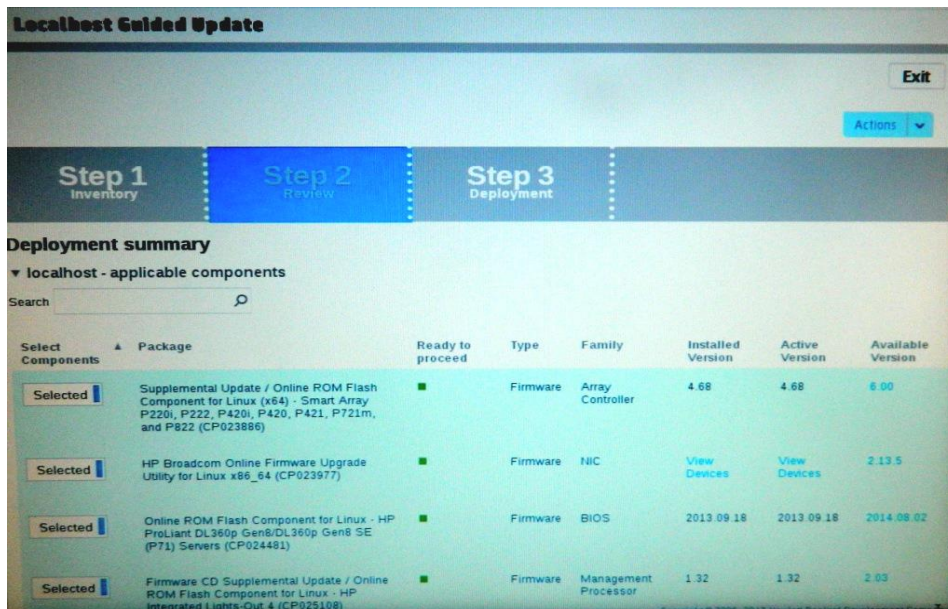
4. HP Interactive Firmware Update will display as shown above.
5. Select English when prompted and press <Continue>
6. Select <Agree> to End User License Agreement



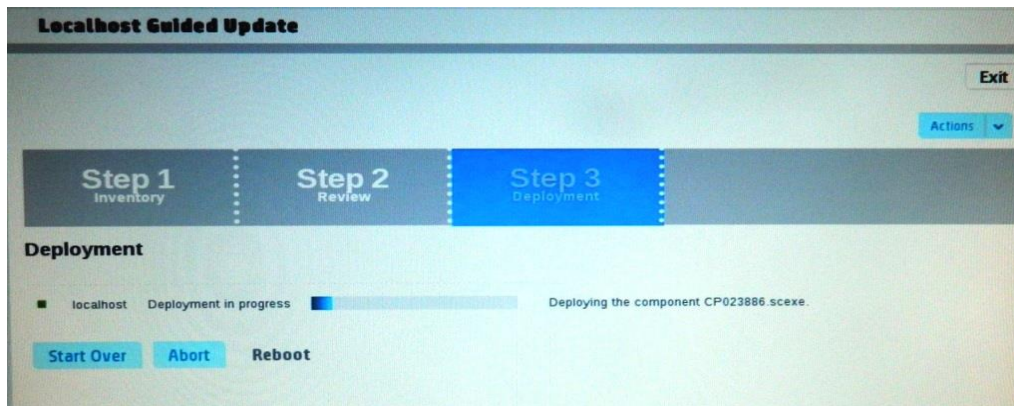
7. Select Firmware Update icon. HP SUM will load. This process will take 4-5 minutes.



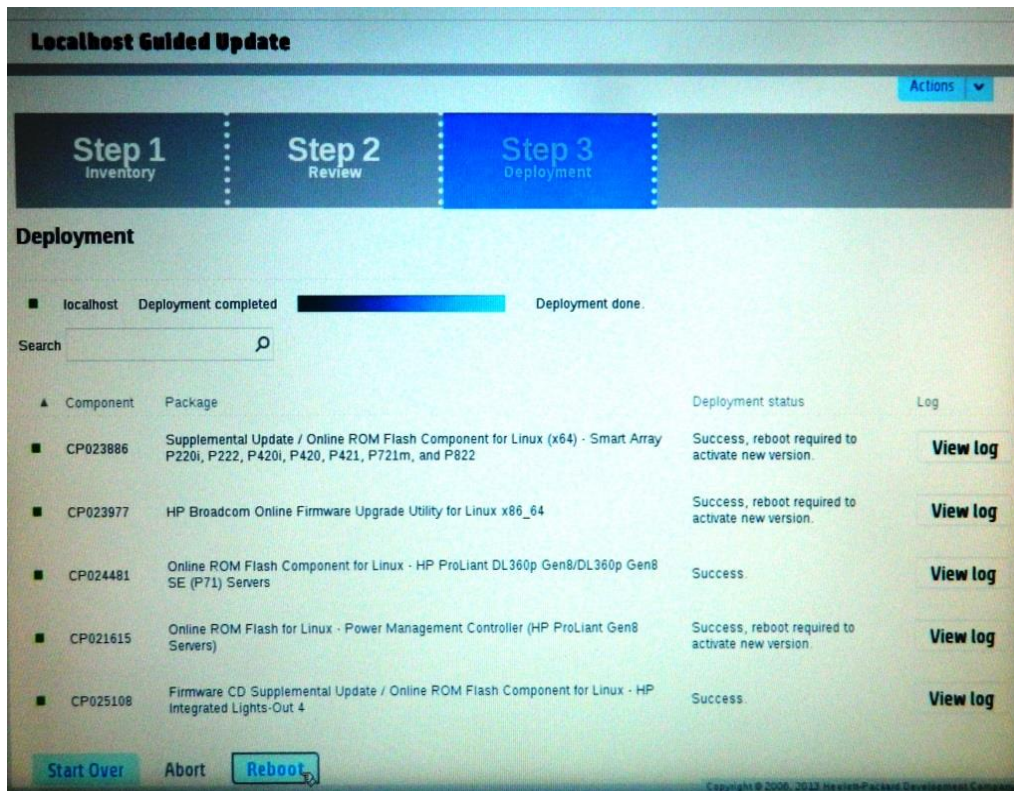
8. An inventory of approximately 25 firmware packages that are suitable to the server will be available for install.
9. Select <Next> when button becomes highlighted.



10. Firmware packages similar to what is shown on the above two screens will display. The tool will auto select (<Selected> button) what packages it determines are necessary for upgrade. Firmware components on the server that are equivalent to or newer than what is on the update disc will not be selected. In this example SMART ARRAY (RAID Controller) will be upgraded from v4.68 to version v6.00. Broadcom NIC devices will be updated to v2.13.5. P71 BIOS will be upgraded from 2013.09.18 to version 2014.09.02. ILO4 will be updated to v2.03 and Power Management Controller will be upgraded to v3.3. HDDs are not selected to update since they match versions on the disc. To see details of the NIC and Power Management controller versions select the <View Devices> text. Firmware rewrites and downgrades can be selected from this menu if needed, but is not detailed in this document. Select <Deploy> when ready to upgrade selected firmware.



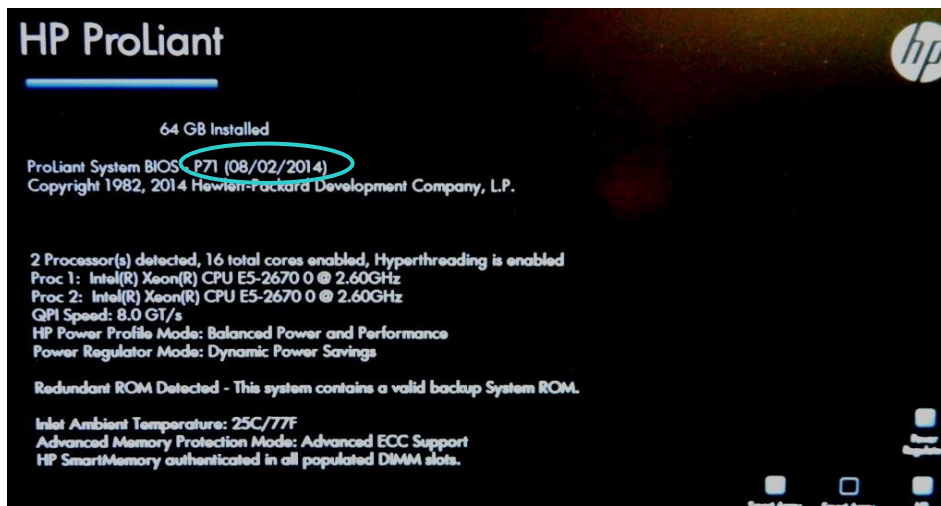
11. Required Updates are being installed



12. When complete, a page will display showing the packages that loaded. If one or more packages did not load successfully select the <View log> button and refer to the section at the end of this document entitled “Update package Error”. If all packages successfully installed select the <Reboot> button. When server starts to boot up (POST) press the DVD drive eject to remove the disc and view new firmware versions reported on the splash screens shown below.

How to check firmware versions on an HP DL360G8.

1. A Monitor and USB keyboard will be required to check firmware versions.
2. Reboot or power up server. Splash screen will appear as shown below.



3. The system BIOS is reported on the first complete line of the HP ProLiant Splash screen. Example: **ProLiant System BIOS – P71 (08/02/2014)**.
4. When the splash screen has progressed to this point press the space bar a couple of times to display additional screens to display iLO 4 and P420i firmware versions. If the user misses pressing the space in time, press **<ctrl> <alt> <delete>** for a server reboot.



5. iLO version (v2.03) is displayed on line 2 of iLO 4 listing and P420i Controller version is displayed on first line of Smart Array Controller.
Example shown above is: iLO v2.03 and P420i v6.00 (RAID Controller).

An alternative to verifying the firmware is to execute the following

System Platform, as root on dom0:

```
# dmidecode | grep "Firmware Revision"
Firmware Revision: 2.3
```

And

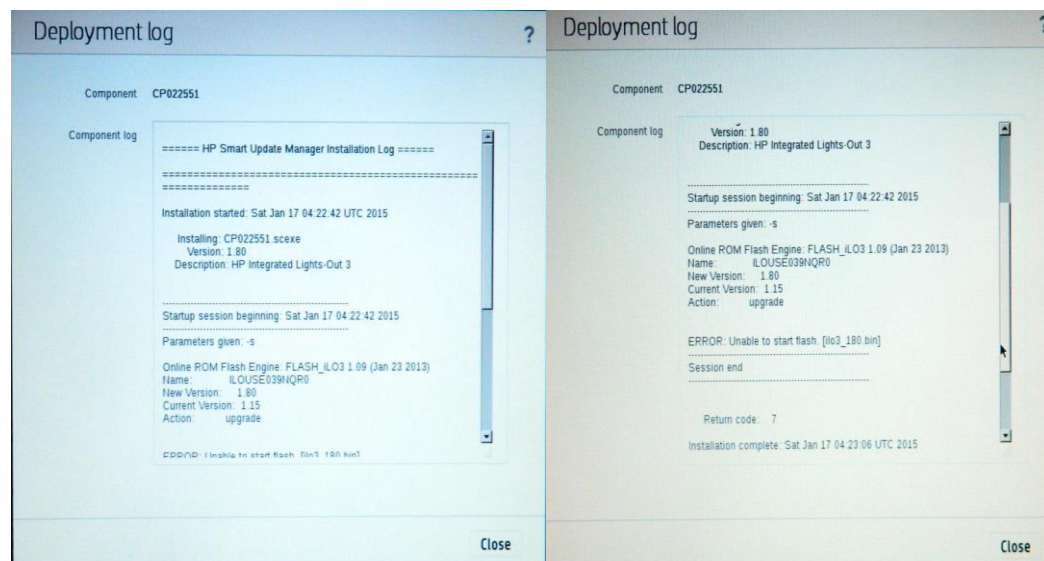
```
[root@cmcpe-meha-dom0a ~]# dmidecode |grep -A 4 "BIOS Info"
BIOS Information
  Vendor: HP
  Version: P71
  Release Date: 08/02/2014
  Address: 0xF0000
```

AVP, as root on AVP:

```
# smbiosDump |grep -A 4 "BIOS Info"
BIOS Info: #0
  Size: 0x00018
  Vendor: "HP"
  Version: "P71"
  Date: "08/02/2014"
```

Update Package Error

If a package did not load successfully select the <View log> button. A dialogue box similar to the ones shown below will display.



View the installation log. It is possible that a prerequisite version of firmware was required to be installed first before the latest package could be installed. If that is indicated in the error log document the log file instructions, including the prerequisite version(s) of firmware required, then proceed with completing the firmware update process to finalize the other successful firmware updates(step 12). Leave the update DVD tool disc in the system throughout the reboot process if the prerequisite version of firmware is found to be on the disc. Check the firmware packages listed on pages 6 and 7 of this document to see if the prerequisite version of firmware is included on this update disc. See next page for how to load prerequisite firmware.

If the called-out prerequisite version of firmware is not listed on pages 6 and 7 of this document and is not displayed on the Deployment Summary Page (See Step 10) notify your AVAYA support contact and report what package is needed as specified from the Deployment log file.

Workaround or alternative remediation

N/A.

Remarks

Issue 2: Added Avaya Aura® Messaging 6.3.x

Issue 3: Added Proactive Contact and necessity for bundled firmware.

Issue 4: Added Avaya Aura® Experience Portal & annotated release strings to include higher versions.

Issue 5: Clarified this is applicable to System Platform 6.3.x and 6.4.x

Issue 6: Added AVP 7.x, removed individual applications that run on System Platform since applicable to any System Platform server 6.3.x and higher.

Patch Notes

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

Backup before applying the patch

N/A.

Download

N/A.

Patch install instructions	Service-interrupting?
N/A.	Yes
Verification	
N/A.	
Failure	
N/A.	
Patch uninstall instructions	
N/A.	

Security Notes

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

Security risks

Cipher Suite 0 vulnerability is resolved by this firmware update. Details of this vulnerability can be found at http://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c03844348

Avaya Security Vulnerability Classification

N/A.

Mitigation

N/A.

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, 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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.