IP Office Technical Tip

Tip Number: **258**

Release Date: **12 December 2013**

Region: **GLOBAL**

Unified Communications Module reverts to “write protect” mode causing Preferred Edition Voicemail to shut down

Avaya has received a number of reports where the Preferred Edition Voicemail has shut down on the Unified Communications Module (UCM). Avaya have conducted a thorough investigation of the issue and established several measures to resolve the issue and minimize customer impact.

This Technical Tip is to inform customers of the issues and the specific actions that should be taken. For further details on the issue please refer to the Product Support Notice (PSN) referenced later in this document.

Problem Description

In certain scenarios, the Solid State Drive (SSD) on the UCM reverts to ‘write protect’ mode as early as a few weeks of use. An affected UCM can shut down the Preferred Edition Voicemail.

Modules affected by this issue can be identified within a serial number range of **13WZ31xxxxxx** and **13WZ43xxxxxx.**

Also, modules exhibiting this issue will have PCS level 9 and PCS level 4 for the on-board SSD. The PCS level for the UCM can be located on either the UCM shipping box (see figure 1) or on the UCM itself (see figure 2). The PCS for the on-board SSD is located on the top right of the blue sticker that is attached to the drive (see figure 3).



Figure 1



Figure 2



Figure 3

Resolution

A PSN is also being issued to address the fault that causes the SSD to revert to "write protect" mode due to a microcontroller firmware deficiency. Other components and performance of the IP Office control unit are not impacted.

The corrective action is to install a Critical Patch (CP) on the UCM through the UCM WebControl Application. The Critical Patch can be found at **http://support.avaya.com**.

The PSN associated with this Technical Tip is **PSN004105**.

This corrective action should be performed on all Unified Communications Modules that meet the serial number and PCS level prerequisites. Failure to perform this corrective action will leave the UCM vulnerable to incorrectly lock into a 'write protect' mode and cause the Preferred Edition Voicemail to shut down. There is a risk of data loss if the unit goes into write protect mode if the procedure is not performed.

Determining if the Critical Patch should be deployed

There are **three** situations that require that the Critical Patch (CP) be installed on the UCM.

1. **UCM installed (no issue):** If the serial number of the installed UCM falls within the range of potentially-affected units, Avaya recommends that the software fix is downloaded and installed on the UCM per the provided instructions.
2. **UCM purchased but not yet implemented:** Avaya recommends that the software fix be downloaded and installed on any existing current non-implemented UCM stock in your inventory.
3. **UCM units that are received coming from Repair/Distribution due to a RMA/DOA replacement:** Avaya recommends that software fix be downloaded and installed on all UCM's that are received from Repair/RMA/DOA replacement.

If your UCM is installed and is currently experiencing this issue the UCM must be replaced. Avaya recommends that our channel partners create an escalation ticket. Partners may elect to follow the RMA/DOA process, if necessary. Additionally, if the customer account has an IP Office Support Services (IPOSS) with Advanced Parts Replacement (APR) contract they can follow the documented IPOSS process.

Critical Patch Installation Instructions for New UCM Deployments

When preparing a new UCM for field deployment you should follow the procedures for igniting the module services and install the current software release ISO image via a USB key **before** you perform the SSD 'write protect' critical patch. These procedures are outlined in the IP Office Unified Communications Module 9.0 Installation and Maintenance Guide (Document 16-601011 Issue 07g) and in the IP Office 8.1 Installation and Maintenance Guide (Document 15-601011 Issue 06g).

The level of software that is pre-loaded on the UCM is identified by the light blue sticker that is placed on top of the SSD drive. In the example below the UCM is running release 8.0.10-3 of software (figure 4):



Figure 4

After the Unified Communications Module (UCM) has been prepared for field deployment you should proceed to apply the SSD Firmware Update Critical Patch.

To perform this firmware update patch you will need:

1. The SSDFWUpgrade-1.0.0-7.zip patch located on the Avaya support web site
2. Access to the UCM WebControl Application

Pre-Installation Instructions

The SSD Firmware Update Critical Patch does not affect the data stored on the SSD. However, Avaya recommends performing a back-up to a remote server if there is customer Voicemail or one-X Portal data residing on the UCM. This should be performed before proceeding with the installation of the SSD Firmware Update Critical Patch.

Critical Patch Installation Instructions for Release 8.1 UCM

1. Launch the WebControl Application and login as Administrator.

2. In the 'Settings' tab, load the zip file in the Applications Software Repositories by browsing to the zip file and then press the 'Add' button.

3. In the 'Updates' tab under the 'Services' window install the new .rpms in the following order:
   a. mailx
   b. smartmontools
   c. SSDFWUpgrade
   Note: The SSD Firmware Upgrade package will NOT install properly if mailx and smartmontools are not installed first

4. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not affect the system

5. The UCM can be restarted via the System Status Application (SSA) (see figure 5) or by pressing the top button on the UCM module.

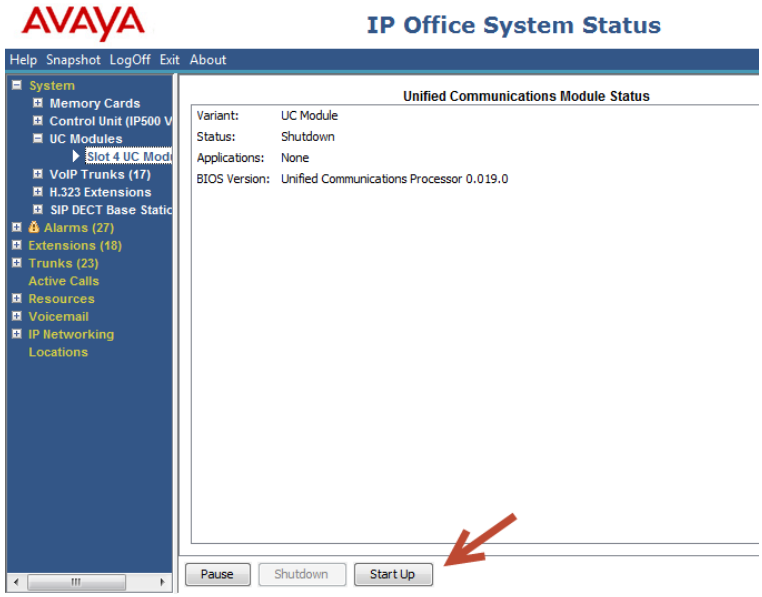


Figure 5

Once the UCM has completed the start-up process the diagnostic information will be displayed in the SSA (see figure 6):

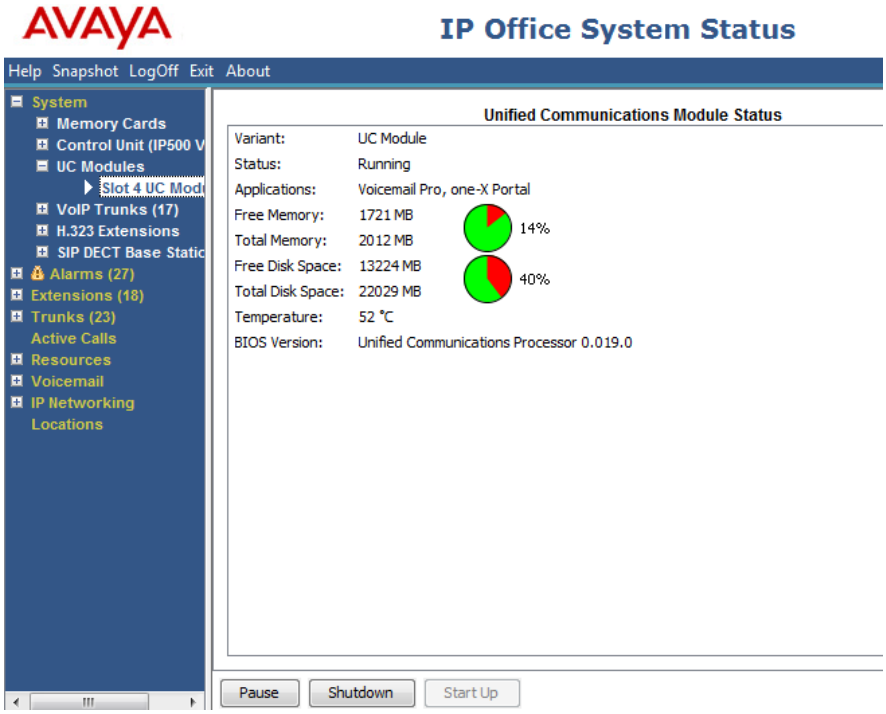


Figure 6

6. The success of the SSD Firmware package can be confirmed by viewing the 'Notifications' window on the WebControl Applications 'Home' tab. This will show one of four possible messages:
    a. 'SSD Firmware not needed. SSD version is Ver703.o'.
    b. 'SSD Firmware not needed. SSD version is S5FAR031'.
    c. 'SSD Firmware upgrade successful. Power cycle was completed to finalize the changes'.
    d. 'SSD Firmware upgrade failed'. **In this case the UCM should be replaced.**

7. At this point the UCM SSD Firmware Upgrade has been completed.

Critical Patch Installation Instructions for Release 9.0 UCM

1. Launch the WebControl Application and login as Administrator.

2. In the 'Settings' tab, load the zip file in the Applications Software Repositories by browsing to the zip file and then press the 'Add' button.

3. Browse to the 'Updates' tab and wait for all of the Services to load.

   There are two possible scenarios for installing the SSDFWUpgrade Critical Patch. This will depend on the method that was used to upgrade the UCM to 9.0 when it was originally installed. If the mailx.rpm and the smartmontools.rpm show that they are 'Up to Date' then you may proceed with the installation of the SSDFWUpgrade by pressing the Install radio button (see Figure 7). Otherwise proceed to step 6.

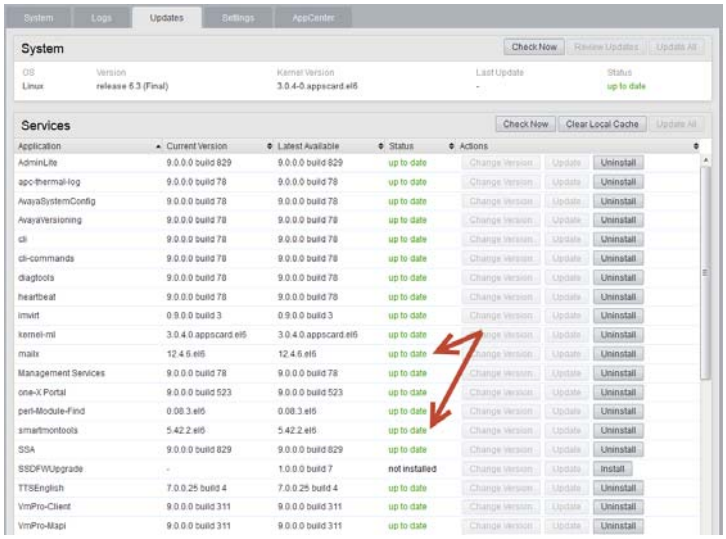


Figure 7

4. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not effect the system and the UCM will not shut down.

5. The UCM can be restarted via the System Status Application (SSA) (see figure 14) or by pressing the top button on the UCM module. Please proceed to step 15.

6. If the mailx.rpm and the smartmontools.rpm show that they are ‘Not Installed’ then you must perform the steps below to correct the corrupted .rpm files on the UCM (see Figure 8):

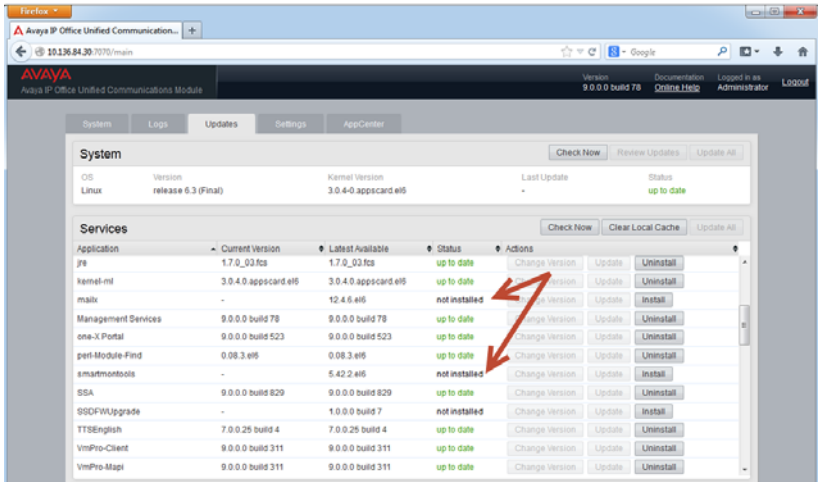


Figure 8

If you attempt to install the mailx and smartmontools from the ‘Updates’ page you will get a Request Error stating the .rpm file is corrupted (See Figure 9):

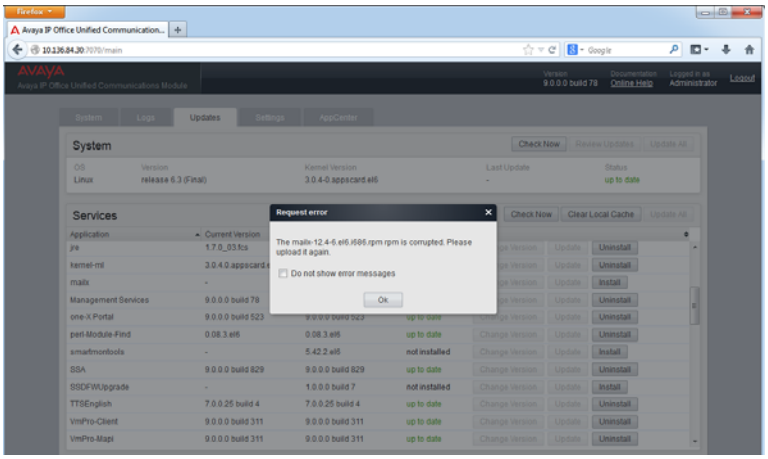


Figure 9

If the mailx.rpm and smartmontools.rpm have been corrupted they can be reloaded to correct the issue. To reload the mailx and smartmontools .rpm files you will need:

a. SSH client (example, PuTTY www.putty.org)
b. Administrator and root access to the UCM
c. WebControl access to the UCM

7. After downloading the PuTTY client you will need to setup PuTTY to access the UCM:
    a. Use the UCM IP Address in the IP address field
    b. The Port should be 22
    c. The connection type should be SSH (see Figure 10)

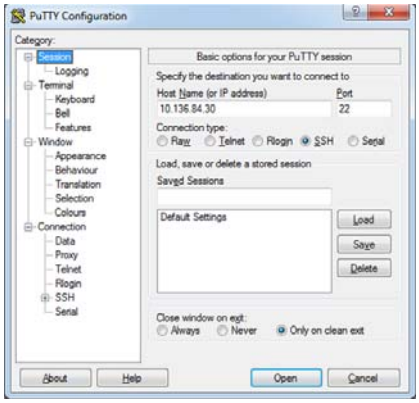


Figure 10

8. Click 'Yes' if you recieve the 'PuTTY Security Alert'. This alert is displayed every time the PuTTY client is trying to access a new system (see Figure 11):

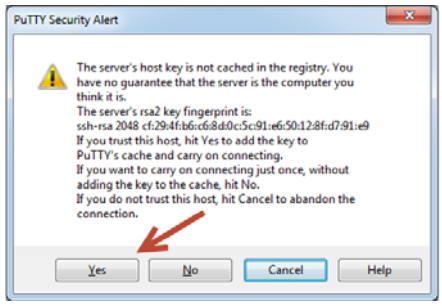


Figure 11

9. Login to the UCM with root access. **Note:** You will need to sign in as 'admin' after you login as the Administrator and before signing in as root. (see Figure 12):

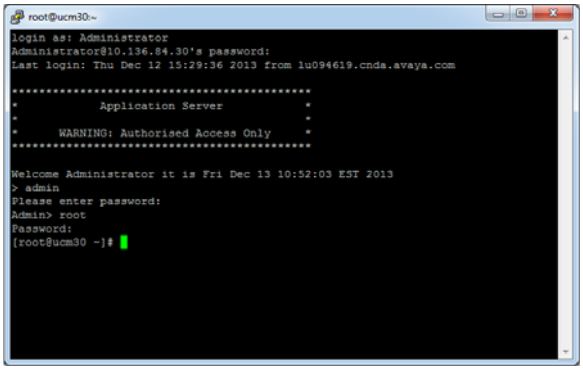


Figure12

10. Type the following command:
    rpm --import /etc/pki/rpm-gpg/* (see Figure 13):

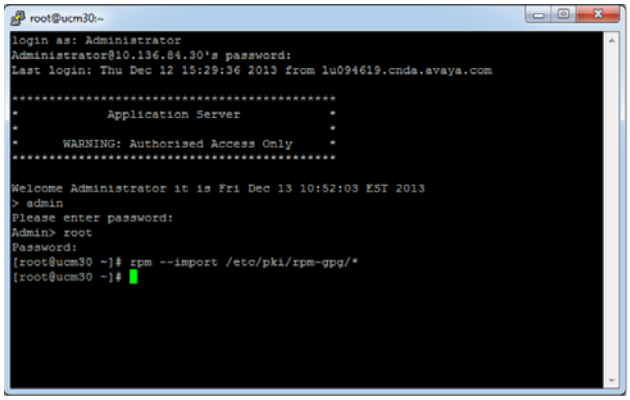


Figure 13

11. Close PuTTy by clicking the ‘X’ button.

12. In the WebControl ‘Upgrades’ Tab, install the ‘mailx’, ‘smartmontools’ and ‘SSDFWUpgrade services in that order. You do not need to reload the zip file.

13. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not effect the system and the UCM will not shut down.

14. The UCM can be restarted via the System Status Application (SSA) (see figure 14) or by pressing the top button on the UCM.

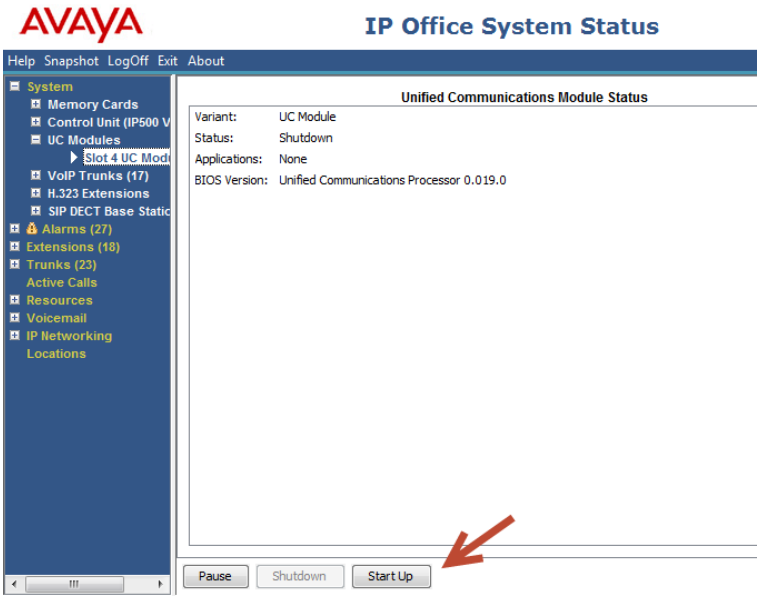


Figure 14

15. Once the UCM has completed the start-up process the diagnostic information will be displayed in the System Status Application (SSA) (see figure 15):

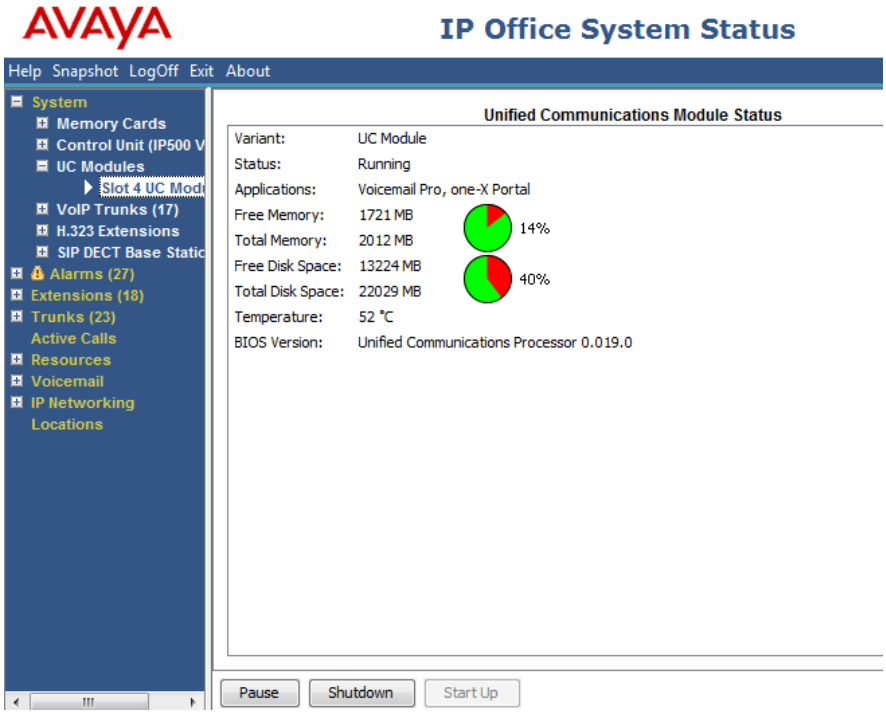


Figure 15

16. The success of the SSD Firmware package can be confirmed by viewing the 'Notifications' window on the WebControl Applications 'Home' tab. This will show one of four possible messages depending on the SSD version installed in the UCM.

    a. 'SSD Firmware not needed. SSD version is Ver703.o'.
    b. 'SSD Firmware not needed. SSD version is S5FAR031'.
    c. 'SSD Firmware upgrade successful. Power cycle was completed to finalize the changes'.
    d. 'SSD Firmware upgrade failed'. **In this case, the UCM should be replaced.**

17. The Unified Communications Module (UCM) SSD Firmware Upgrade has been completed.

SSD Firmware Package Upgrade – FAQ's

What can happen if I choose not to install the SSD Firmware Package Upgrade?

The corrective action should be performed on all Unified Communications Modules that meet the serial number and PCS level prerequisites. Failure to perform this corrective action will leave the UCM vulnerable to incorrectly lock into a 'write protect' mode and cause the Preferred Edition Voicemail to shut down. There is a risk of data loss if the unit goes into write protect mode if this procedure is not performed.

How long does the SSD Firmware Package Upgrade take to complete?

On most drives the upgrade takes less than 3 minutes to complete.

Is the SSD Firmware Package Upgrade service effecting?

Yes but this is limited to the UCM and services. The Voicemail Pro and the one-X Portal applications will have to be restarted. After the SSD Firmware Package completes the UCM will power down and must be restarted from the SSA or manually pressing the top button on the UCM Module. All other call processing continues during the SSD Firmware upgrade, the IP500v2 system unit does not need to be restarted for the Firmware upgrade to take effect.

The UCM is installed in an active IP500v2 and I cannot take the system down to check and see if the UCM meets the serial number and PCS prerequisites. Should I attempt to install the SSD Firmware Upgrade package anyway?

Yes. The script will determine if the SSD Firmware Upgrade is required. For cases where the upgrade is not required, the attempted installation of this upgrade package does not affect the system.

Can I use the upgrade.zip file instead of the full installation image (.iso) file to upgrade a UCM from 8.0 to either 8.1 or 9.0 or from 8.1 to 9.0?

No. You must use the full installation image (.iso) and the USB Initiator method to upgrade between major releases. The 'upgrade.zip' file can only be used to upgrade within the same release. For example, you can use the 'upgrade.zip' file to upgrade from 8.1(x) to 8.1(y).

Issued by:
Avaya SMEC Customer Product Engineering Support

Contact details:-
EMEA/APAC

*Email: **gsstier4@avaya.com***

NA/CALA

*Email: **IPONACALAT4@Avaya.com***

*Internet: **http://www.avaya.com***
© 2013 Avaya Inc. All rights reserved.