Product Support Notice

© 2017 Avaya Inc. All Rights Reserved.

PSN #	PSN004806u

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

Original publication date: 18-Sep-17. This is Issue #01, Republished date: N/A

Severity/risk level	High	Urgency	Immediately

Name of problem Patch 1 for System Manager 7.0.1.3 release

Products affected

Avaya Aura® System Manager: Release 7.0.1.3

Problem description

Note: If you have installed System Manager 7.0.1.3 Software it is highly recommended that you apply this hot fix if you have not installed one already since you may run into issues with the /opt/ partition filling up which may cause impact.

Following is the list of issues fixed in Patch 1 for System Manager Release 7.0.1.3:

1. Cannot upload Announcement on AMS 7.8.0.240 via System Manager Web UI
2. CM Notify Sync feature does not work properly if there are more than 18 CM's configured for notify sync on System Manager.
3. Announcement file path is prefixed with incorrect file path while uploading Announcements via System Manager Web UI
4. Unable to create CM templates via the Manage Endpoints page if the station has values for Floor, Building under Site Data tab and AUDIX name under Feature Option
5. Unable to repair the Serviceability Agent for Primary / Secondary System Manager via the web interface in release 7.0.x.x
6. Selecting multiple serviceability agents (more than 10) and repairing them all at the same time causes the alarming page to stop working.
7. CPU alarming not working in certain scenarios.
8. Upgrade from OOBM enabled 7.0.1.3 System Manager to 7.1.1 fails.
9. Upgrade third party component Trinidad to 1.2.13 to fix a memory leak with the older version.
10. Analyze operation may not work in some cases due to failure to remove the Analyze lock file.
11. List vdn report does not show skill data properly.
12. PROP7.0.1: Patch Manager shows as "ready to install" patches which are not applicable to selected platform.
13. /opt/ partition filling up with log file causing System Manager to not function properly.
14. Unable to import users post DST change if the data has timezone prior to DST change.
15. No audit logs are generated when users are permanently deleted from User Management.
16. Not able to import CA certificate without CN into System Manager trust store

Resolution

System_Manager_7.0.1.3_Patch1_r701307037.bin will fix the above mentioned problems in System Manager 7.0.1.3 Release. See the patch notes below on how to download and install the required patch.

Workaround or alternative remediation

n/a

Remarks

This patch must be applied on System Manager 7.0.1.3 release or 7.0.1.3 + hot-fix release

To determine the System Manager 7.0.1.3 release that is running:

- Log on to the System Manager Console.
- On the top-right corner click on the  icon and then select the "About" link. Verify that About page contains as below: **System Manager 7.0.1.3**

Patch Notes

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

Backup before applying the patch

Recommended

Download

Follow the instructions below to download the patch:

1. Go to http://support.avaya.com
2. Click on "Downloads & Documents" link on the dashboard menu.
3. Enter product name as "system manager" and then select "Avaya Aura® System Manager"
4. Select "7.0" from the Choose Release dropdown
5. Click on "Avaya Aura® System Manager Release 7.0.1.3 Downloads".
6. Click on the file "System_Manager_7.0.1.3_Patch1_r701307037.bin" to download.

Alternately you may also use PLDS download ID "SMGR7013005" to download the file directly from PLDS.

Patch install instructions

Service-interrupting?

Yes. During the patch installation the System Manager services (web access to System Manager) will be disrupted for approximately 30+ minutes.

IMPORTANT: If System Manager installation is a Geo-Redundancy enabled deployment, Geo-Redundancy should be disabled, the patch should be applied to both Primary and Secondary System Manager systems, and then re-enable Geo-Redundancy.

Note: This patch **MUST** be applied on Avaya Aura® System Manager 7.0.1.3.

Follow the instructions below to install the patch through System Manager CLI for Virtualization Enablement (VMWare) environment or Avaya Virtualization Platform based deployment:

1. Take a snapshot of System Manager virtual machine.
   Note: This activity might impact the service.
2. Copy the patch installer file (System_Manager_7.0.1.3_Patch1_r701307037.bin) to the System Manager server.
3. Log in to the System Manager virtual machine as root user.
4. Verify md5sum of the bin file with the value mentioned on PLDS (3709df48cd1369f7588c58b9293c6cb9)
5. Run the patch installer using the following command:
   #SMGRPatchdeploy <absolute path to System_Manager_7.0.1.3_Patch1_r701307037.bin file>
   Note: you will be prompted to accept the EULA. You must accept the EULA in order to install the patch.
6. Wait for the system to execute the patch installer and display the installer prompt.
7. Log on to System Manager Console, and verify whether the System Manager UI is displayed correctly.
   - On the top-right corner click on the  icon and then select the "About" link. Verify that the system displays the version information in the following format:
     System Manager 7.0.1.3
     Build No. - 7.0.0.0.16266
     Software Update Revision No: 7.0.1.3.097037
     Service Pack 3
8. Remove the snapshot taken in step #1 once all functionality has been verified.
   Note: This activity might impact the service.

Verification

To verify the successful installation Patch:

- Log on to System Manager Console.
- On the top-right corner click on the  icon and then select the "About" link. Verify that the system displays the version information in the following format:
  System Manager 7.0.1.3
  Build No. - 7.0.0.0.16266
  Software Update Revision No: 7.0.1.3.097037
  Service Pack 3

Failure

In case of issues with the patch, you can:

1. Retry the action. Carefully follow the instructions in this document.
2. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any

© 2016 Avaya Inc. All Rights Reserved.

and the release version in which the issue occurs

Patch rollback instructions

If System Manager is on VMWare deployment, revert the snapshot taken prior to patch installation.

In case if you still have issues with the patch rollback, you can:

1. Contact Avaya Support, with following information: Problem description, detailed steps to reproduce the problem, if any and the release version in which the issue occurs

Note: if a snapshot was not taken prior to attempting to install the patch then rollback will require performing a cold standby procedure using the last good backup.

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

Not Susceptible

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 unless otherwise specified in the Avaya support Terms of Use.

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 DAMA GES 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 TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.