



Product Support Notice

PSN # PSN005568u

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

Original publication date: 07-March -2022. This is Issue #01,
Published date: 07-March -2022.

Severity/risk level

Medium

Urgency

When convenient

Name of problem PSN005568u - System Manager 10.1.0.0 Hot Fix 1

Products affected

Avaya Aura® System Manager: Release 10.1.0.0

Problem description

PSN Revision history:

Issue #1 – PSN originally published on 4th March 2022

This PSN releases System_Manager_R10.1_GA_HotFix1_r101014254.bin file.

Important Notes:

- Please ensure that you read through the entire PSN carefully, especially the Patch Installation section, before starting with the Patch install.
- This Hot Fix patch can ONLY be installed on a System where the mandatory System_Manager_10.1.0.0_GA_Patch2_r101014119.bin has been installed.
- System Manager Hot Fixes are cumulative unless stated otherwise. What this means is if you received a System Manager 10.1 GA hot fix previously, then this hot fix contains all those fixes as well unless stated otherwise.

Note for Avaya Services Team: Please see R2 version of this PSN for JIRA numbers associated with the issues mentioned below.

Following are the issues fixed in System_Manager_R10.1_GA_HotFix1_r101014254.bin.

1. Unable to extract IP Office upgrade related files via System Manager SDM
2. Unable to migrate CM and BSM running on Avaya Solutions Platform (ASP) S8300 R5.1 card to 10.1.x
3. Unable to Generate certificate for ASP 130 R5.x and ASP S8300 R5.1 using SDM client and SMGR SDM
4. IP Network Map entries not showing up in SMGR even though it's programmed in Communication Manager
5. Unable to deploy CM 10.1 on ASP S8300 R5.1 using System Manager SDM

Resolution

System_Manager_R10.1_GA_HotFix1_r101014254.bin will fix the above-mentioned problems in System Manager 10.1.0.0 release. See the patch notes below on how to download and install the patch

Workaround or alternative remediation


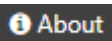
n/a

Remarks

Patch must be installed on top of System Manager 10.1 GA. You are considered to be on 10.1 GA only if you installed System_Manager_10.1.0.0_GA_Patch2_r101014119.bin. For details on System_Manager_10.1.0.0_GA_Patch2_r101014119.bin see PSN005566u.

Installation of this Patch is Service impacting from a System Manager standpoint.

To determine whether System Manager 10.1.0.0 GA release is installed:

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

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. Under the “Support by Product” menu click on “Downloads”
3. Enter product name as “system manager” and then select “Avaya Aura® System Manager”
4. Select “10.1.x” from the Choose Release dropdown
5. Click on “Avaya Aura® System Manager Release 10.1 Downloads, 10.1.x”.
6. Click on the file “System_Manager_R10.1_GA_HotFix1_r101014254.bin” to download.

Alternately you may download the file directly from PLDS using PLDS download ID “SMGR101GAHF1”.

Note: It takes a few days for the Patch download link to show up on the Avaya Support site. Please use PLDS during that time to download the patch.

Patch install instructions

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. You should apply the patch on the System Manager servers one a time. Do not install the patch on both primary and secondary System Manager servers at the same time.

Note1: This patch **MUST** be applied on Avaya Aura® System Manager 10.1.0.0 GA load.

Note2:

Patch must be installed on top of System Manager 10.1 GA. You are considered to be on 10.1 GA only if you installed System_Manager_10.1.0.0_GA_Patch2_r101014119.bin. For details on System_Manager_10.1.0.0_GA_Patch2_r101014119.bin see PSN005566u.

Service-interrupting?

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

Follow the instructions below to install the patch through System Manager CLI for Virtualization Enablement (VMWare) environment or Avaya Virtualization Platform based deployment. The instructions for installing the patch on primary and secondary System Manager are the same.


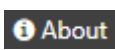
1. Disable System Manager Geo redundancy if your System Manager is deployed as a Geo redundant System. It is important that you disable Geo prior to taking snapshots to avoid issues that might arise due to postgres WAL segments after you revert the snapshot.
2. Take a snapshot of System Manager virtual machine.

Note: This activity might impact the service.

3. Copy the patch file (System_Manager_R10.1_GA_HotFix1_r101014254.bin) to the System Manager server under the /swlibrary/ folder
4. Log in to the System Manager virtual machine command line using the user that was set up during 10.1 OVA installation.
5. Verify md5sum of the bin file with the value mentioned on PLDS
(**1e8b50084466a1ef324dcee949a581be**)
6. Run the patch installer using the following command:
#SMGRPachdeploy <absolute path to System_Manager_R10.1_GA_HotFix1_r101014254.bin file>

Note: you will be prompted to accept the EULA. You must accept the EULA to install the patch.

7. Wait for the patch execution to complete.
8. 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 click the  About link. Verify that About page contains as below:

System Manager 10.1.0.0

Build No. – 10.1.0.0.537353


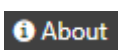
Software Update Revision No: 10.1.0.0.0614254

Note: The value for Security Mode on your system may defer depending on the Security Profile that you are running. “Standard Hardening” is the default Security Mode.

9. Install the Hot Fix on the Geo Redundant System Manager if you have one – follow steps 2 through 8 mentioned above for the patch installation.
10. Remove the snapshot taken in step #1 once all functionalities have been verified.
Note: This activity might impact service.
11. Enable Geo Redundancy if you have Geo Redundant System Manager deployment.

Verification

To verify the successful installation Patch:

- On the top-right corner click on the  icon and then click the  About link. Verify that About page contains as below:

System Manager 10.1.0.0

Build No. – 10.1.0.0.537353

Software Update Revision No: 10.1.0.0. 0614254

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 and the release version in which the issue occurs.

Patch rollback instructions

If System Manager is deployed on a virtualized environment, revert the snapshot taken prior to patch installation. Note: snapshots are the only way to revert / uninstall the patch.

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.

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