Product Support Notice

PSN #	PSN005269u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 10-May-2019. This is Issue #02 Published date: 14-June-2019		Severity/risk level	High	Urgency	Immediately
Name of problem	Patch 2 for System Manager 8.0.1.1 Release				

Products affected

Avaya Aura® System Manager: Release 8.0.1.1

Problem description

Important Note:

- This PSN is being republished on 14th June 2019 to release System Manager 8.0.1.1 Patch 2
- System Manager 8.0.1.1 Patch 2 is cumulative of System Manager 8.0.1.1 Patch 1
- Patch 1 has been removed from PLDS and the support site and if you need Patch 1 for any reason please reach out to the Avaya Support team.

Following are the issues fixed in System Manager 8.0.1.1 Patch 2 (in addition to the ones that are already there from Patch 1):

1. Messaging Element Manager Fixes
2. Coverage Path is set to blank for a station when creating a user even when it is configured in UPR using a custom CM template.
3. User creation fails when using UPR if the UPR uses a CM endpoint template that has a value configured for voicemail.
4. Coverage path gets removed from a station when “use existing station” option is used for creating the user with CM comm profile
5. System Manager displays wrong name of Department when viewing a User with OfficeLinx comm profile
6. Breeze Element Manager Fixes
7. “Block New Registration When Maximum Registrations” and “Enable Centralized Call History” fields are not taken when creating a user using a UPR that has those values set in it.
8. Advance Search option does not work from the Manage Endpoints or Agents page after upgrade to 8.0.1
9. Autocomplete does not work for the location field in the SM comm profile
10. Preferred Handle does not get updated in the CM comm profile
11. CM comm profile cannot be unassigned from a user if the extension is part of Coverage Answer Group
12. Unable to edit a user if the user has a handle of type “Other XMPP” added to it.

Following are the issues fixed in System Manager 8.0.1.1 Patch 1:

1. Clicking on Certificate renewal Button does not redirect proper page.
2. XML Parsing Error After Clicking on Create New Button on Coverage Path Page.
3. Migrating CM 6.3 (System Platform based deployment) using SDM does not create UPGRADE job.
4. Edit operation of Upgrade Configuration failure on Save.
5. Firewall Changes to support ED application
6. Customer cannot configure **9911 as an emergency number.
7. Blank page when user tries to EDIT / VIEW coverage path.
8. ovf-env-smgr.txt file does not have correct permissions this further causes when user tries to upgrade System Manager from SDM Client. The configuration page does not pre-populate the existing System Manager values.
9. Upgrade of Media module of MG gets stuck in the pending state.
10. Not able to add ADA MGC in System Manager, users get error - "Attribute name Companding law not found".
11. Filling up the secure store table to the extent that it causes Geo workflow to fail.
12. Officelinx profile doesn't display when creating Officelinx user using "Provision User Rule" in case "Department" field isn't selected.
13. Refresh Element job does not finish when elements of different types are selected.
14. After clicking on "Migrate with AVP install" checkbox new tab is not displayed while migrating from System Platform to AVP.
15. Unable to access Elements ->Meeting Exchange link from System Manager Web console

Resolution

System_Manager_R8.0.1.1_HotFix2_r801109857.bin will fix the above-mentioned problems in System Manager 8.0.1.1 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 8.0.1.1 or any other previous 8.0.1.1 hot fix that you may have installed on the system. This patch contains all fixes that were delivered in the previous patches / hot fixes.

To determine whether System Manager 8.0.1.1 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:

  System Manager 8.0.1.1

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 "8.0.x" from the Choose Release dropdown
5. Click on "Avaya Aura® System Manager Release 8.0.1.1 Downloads".
6. Click on the file "System_Manager_R8.0.1.1_HotFix2_r801109857.bin" to download.

Alternately you may download the file directly from PLDS using PLDS download ID "SMGR8011GA6"

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.

Note: This patch **MUST** be applied on Avaya Aura® System Manager 8.0.1.1 load.

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. Take a snapshot of System Manager virtual machine.

   Note: This activity might impact the service.
2. Copy the patch installer file (System_Manager_R8.0.1.1_HotFix2_r801109857.bin) to the System Manager server under the /swlibrary/ folder
3. Log in to the System Manager virtual machine command line using the user that was set up during 8.0 OVA installation.
4. Verify md5sum of the bin file with the value mentioned on PLDS (77d97ae2e83229619eff9ed48fe2e3fd)
5. Run the patch installer using the following command:

   #SMGRPatchdeploy <absolute path to System_Manager_R8.0.1.1_HotFix2_r801109857.bin file>

   Note: you will be prompted to accept the EULA. You must accept the EULA to install the patch.
6. Wait for the system to execute the patch.
7. Log on to System Manager Console and verify whether the System Manager UI is displayed correctly.

Service-interrupting?

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

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

  System Manager 8.0.1.1
  Build No. - 8.0.0.0.931077
  Software Update Revision No: 8.0.1.1.039857
  Service Pack 1

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.

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:

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

  System Manager 8.0.1.1
  Build No. - 8.0.0.0.931077
  Software Update Revision No: 8.0.1.1.039857
  Service Pack 1

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 on VMWare deployment so 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.

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.