Product Support Notice

© 2022 Avaya Inc. All Rights Reserved.

PSN # PSN005887u

Original publication date: 28-Apr-2021. This is Issue #04, published date: 16-Dec-2022. Severity/risk level Medium Urgency When Convenient

Name of problem Field Alert – AWE 20.1 and AWE 15.2.X Localization (L10n) Update installation procedure.

Products affected

Avaya Workforce Engagement 20.1 and Avaya Workforce Engagement 15.2.X

Problem description

AWE Localization (L10n) updates are provided with KBs. The Three KBs are usually presented as a zip file on Avaya PLDS. The constituent KB components are:

- L10n framework apps flatfiles.
- L10n framework BPmainDB.
- L10n framework apps staticfiles.
- Additionally, the L10n online helpfile is available.

Recent updates of the three L10n update KBs now require an additional command line step to install the KBs.

Problem Summary.

AWE Localization KB updates which are in .msi format require an additional command line step to ensure installation on top of older Localization (L10n) installation. The additional command line option overwrites the dependency that prevented installing the latest KBs directly on top of the Gray package, which may have been applied on a previously installed Green package, or top of previously provided Localization (L10n) KB updates.

Affected Product Versions.

- AWE 15.2.X
- AWE 20.1

L10n framework apps flatfiles

- Dependencies
  - None
- Affected Server Role(s)
  - Framework Applications
- Affected Platform(s)
  - Consolidated
  - Data Center
  - Application
- Downtime
  - Applications Only

L10n_framework_BPmainDB

- Dependencies
  - None
- Affected Server Role(s)
  - Framework Database
- Affected Platform(s)
  - Consolidated
  - Data Center
  - Database
  - Framework Database & Reporting
  - Framework Database
- Downtime
  - Applications Only

L10n_framwork_apps_staticfiles

- Dependencies
  - None
- Affected Server Role(s)
  - Framework Applications
- Affected Platform(s)
  - Consolidated
  - Data Center
  - Application
- Downtime
  - Applications Only

L10n on line help file

- Dependencies
  - None
- Affected Server Role(s)
  - Framework Applications
- Affected Platform(s)
  - Consolidated
  - Data Center
  - Application
- Downtime
  - Applications Only

Resolution

Installing KB's

The following steps must be performed as an Admin user for each of the four KBs (with respect to Dependencies, Server Role and Platform mentioned in the Problem Description section above:

1. Login with the management service account and copy the KBXXXXXX.msi file into a local folder, e.g C:\ KBXXXXXX.msi
2. Open a DOS Command window with Admin rights and navigate to the local folder, where you have placed the MSI.
3. To install each KB (patch msi), run the msiexec command:
   msiexec /i KB<num>.msi ALLOWGREEN=1 (If you want to log you will need to add /L*V "C:\PATH TO YOUR .log" before ALLOWGREEN=1)
   where <num> is the version number of the KB.
   For example:

```
C:\Users\ap2admin>cd C:\Users\ap2admin\Desktop\KB's

C:\Users\ap2admin\Desktop\KB's>msiexec /i KB181269-15.2.7.857.msi ALLOWGREEN=1
```

4. Type msiexec /i and press TAB, to cycle through the KBs.
5. Run the installer for each KB.
6. Patchlog.txt contains installation logs.
7. Wait until MSI is done, then click the "Finish" button
8. Once you have performed these steps for all the KBs, restart the machine or Weblogic.

Verification

Verify installation from Control Panel > Add Remove program. You will find an entry with KBXXXXXX.

Rollback

From Add/Remove Programs, uninstall the KBXXXXXX.

Workaround or alternative remediation

n/a

© 2022 Avaya Inc. All Rights Reserved.

Remarks

References:

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

PLDS ID WFO000001103.

Patch install instructions	Service-interrupting?
As per the Problem Description section above.	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

Avaya Security Vulnerability Classification

Not Susceptible

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, the 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.

© 2022 Avaya Inc. All Rights Reserved.