

PSN # PSN006256u

Original publication date: 29-Jan-2024. This is Issue 01, published date: 29-Jan-2024.

Severity/risk level

Medium

Urgency

Optional

Name of problem

IP Office Subscription K8s Maintenance Window Update Feb-2024

Products affected

IP Office Subscription Offer

Description

This document provides detail of the maintenance window scheduled for updating the cloud components within the IP Office Subscription Cluster, for each geographic region.

Schedule

Project	Cluster Zone	MW Duration	Date	Local time (Cluster Zone time)
Subscription -NA1	us-east1	4 Hours	Feb-9-2023	11:00 PM to 3:00 AM EST (Eastern Standard Time)
Subscription -NA2	us-central1	4 Hours	Feb-12-2023	10:00 PM to 2:00 AM CST (Central Standard Time)
Subscription -UK1	europa-west2	4 Hours	Feb-13-2023	4:00 AM to 8:00 AM WET (Western European Time)
Subscription -EU1	europa-west6	4 Hours	Feb-14-2023	5:00 AM to 9:00 AM WEST (Western European Summer Time)
Subscription -APAC1	asia-southeast1	4 Hours	Feb-15-2023	12:00 PM to 4:00 PM SST (Singapore Standard Time)
Subscription -EU2	europa-west3	4 Hours	Feb-16-2023	5:00 AM to 9:00 PM WEST (Western European Summer Time)

Components updated during Maintenance Window

The following components may be included in any maintenance window update:

1. Google Cloud infrastructure
2. IP Office common components such as CAS, COM, CSI, etc.
3. Phone binaries (Avaya IX Workplace & Vantage)
4. IP Office software images

Impact on services during the Maintenance Window update

1. IP Office licenses may move into grace mode for a short duration during the update time frame and subsequently phones may show a "License expired" message. The licenses will become available again once the update is complete with no action needed by the end user.
2. IP Office Upgrades Backup/Restore, Logs Management from COM will fail if running during the update.
3. Remote log capture using Sysmon will stop and will resume once the update is complete, with no action needed from the end user.

4. Remote IP Office monitoring using SSA will stop and the end-user will need to reconnect SSA once the update is complete.
5. Remote management (Over COM proxy), will not be available during the update or may be disconnected multiple times during the update.
6. Remote connection to IP Office over SSH, RDP, and HTTPS will not be available during the update.

The following services will not be impacted

1. Telephony Operations.
2. Local access to administration and user applications such as Web Manager, User portal, etc.
3. Local log capturing using Sysmon.
4. Local IPO monitoring using SSA

Recommendation: Don't make any IP Office configuration changes during the maintenance window updates.

Limitations:

N/A

Resolution

Above listed limitations would be enhanced in future releases.

Workaround or alternative remediation

N/A

Remarks

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

n/a

Patch install instructions

Service-interrupting? N

n/a

Verification

n/a

Failure

n/a

Patch uninstall instructions

Service-interrupting?

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 LLC, 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 LLC.
All other trademarks are the property of their respective owners.