Product Support Notice

PSN #	PSN006211u				
Original publication date: 13- Sep-2023. This is Issue 01, published date: 13-Sep-2023.		Severity/risk level	Medium	Urgency	Optional

Name of problem

IP Office Media Manager failed upgrades from 11.0.4.x to 11.1.x

Products affected

IP Office Media Manager

Description

After upgrading from IP Office 11.0.4.x -> 11.1.x, Media Manager runs an automatic process to update the call recordings database and encrypt it. The update process must not be interrupted by a manual Media Manager service stop or IP Office Server Edition server restart. Following successful completion, the Media Manager will start automatically with the old call data and start to pickup the calls that were recorded by the Voicemail Pro service since server post migration start-up.

Resolution

For R11.1, Media Manager encrypts all call details in its call recording database, previously these were unencrypted. As part of that process, Media Manager needs to complete the post upgrade process described above. Depending on the number of recordings and the server resources, this process may take several hours. For example, a system with a million call recordings the process has been known to take approximately 10 hours.

During the update process to ensure it is successful, it is essential that no operations are performed that may affect Media Manager, such as service or server stop/restart. You must wait for the Media Manager service to be fully operational**.** Any interventions to the transient **Media Manager** may trigger the initialization of a new database at startup and consequently a failure of the upgrade. To avoid this issue please follow the process below.

- Please stop the Media Manager service before the IP Office upgrade and do not set it to auto start.
- Note that this does not affect call recording for calls during this time, as that function is performed by the Voicemail Pro service. However, it is advisable that sufficient hard drive free space is made available to allow the Voicemail Pro service to record all calls during the database encryption process. VMPro already has a 20 GB quota for VRL Recordings. This is typically 4000 hours of Opus recording. However, if the size or your calls database is bigger then 1,6 million entries then you can change the quota by editing the file “/etc/vmpro_settings.ini” and the field to be modified is “VRLQuota”. This additional allocated capacity specified must also be available in the free physical Hard Drive. Restart the Voicemail Pro service after editing the file. Please restore the default value in the first available maintenance window.
- Following successful upgrade of all the other IP Office components, next re-start the Media Manager service post server upgrade to 11.1 is complete. This will trigger the post-upgrade encryption process.
- Completion of the post-upgrade process is indicated by the Media Manager successfully starting up. It also will be appearing in WebManager->Applications
    - There is also a log file(/opt/MediaManager/log_encrypt_migration.txt) which provides some data about the upgrade process like below:
        - totalRecords 69812[Number of records to be updated]
        - 241800[Time taken in Milliseconds]
        - All record updated [Indicating the process is complete]

- If the process is interrupted for some reason and Media Manager goes into an inconsistent state, please following the following steps for recovery:
    - Restore the 11.0 Media Manager Backup on the 11.1 System
    - The Restore automatically restarts the database encryption process. Allow the process to continue until completed.

.

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.