



# Product Support Notice

© 2017 Avaya Inc. All Rights Reserved.

PSN # PSN020280u

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

Original publication date: 25-Jan-17. This is Issue #01, published date: 25-Jan-17. Severity/risk level Medium Urgency When convenient

Name of problem The Coaching Intrusion and Whisper Paging features should not be used with digital endpoints.

### Products affected

1400 Series Digital Deskphones

1403 codes 700469927; 700508193

1408 codes 700469851; 700500202; 700504841; 700510909

1416 codes 700469869; 700508194; 700510910

9400 Series Digital Deskphones

9404 codes 700500204; 700508195

9408 codes 700500205; 700504680; 700508195; 700508255

9500 Series Digital Deskphones

9504 codes 700500206; 700501978; 700508197; 700508256; 700510914

9508 codes 700500207; 700500208; 700501979; 700504842; 700508257; 700510913

### Problem description

When Coaching Intrusion is used with 1400/9500 series digital endpoints, connected to IP Office, using a headset that is directly connected to the endpoint via a HIC-1 cord, the “coach” audio might be heard by the far end listener instead of just the agent that is being “coached”.

When Whisper Paging is used with 1400/9400 series digital endpoints, connected to CM, using a headset that is directly connected to the endpoint via a HIC-1 cord, the “whisper pager” audio might be heard by the far end listener instead of just the agent/extension that is being “paged”.

### Resolution

The Coaching Intrusion feature is only supported with IP endpoints connected to IP Office.

The Whisper Paging feature is only supported with IP endpoints connected to CM.

### Workaround or alternative remediation

n/a

### Remarks

n/a

## 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

n/a

### Service-interrupting?

No

### 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

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](http://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 ™ are registered trademarks or trademarks, respectively, of Avaya Inc.  
All other trademarks are the property of their respective owners.