



Product Support Notice

© 2023 Avaya LLC All Rights Reserved.

PSN# PSN006202u

Original publication date: June 30, 2023. This is Issue #01, publication date: June 30, 2023.

Severity/risk level

Medium

Urgency

When convenient

Name of problem

Microsoft announced retirement of Azure AD Graph API support after June 30th 2023

Products affected

Avaya Aura Device Services

Problem description

This PSN advises customers and partners of the upcoming EoS for Azure AD Graph API announced by Microsoft.

[Azure AD: Change Management Simplified - Microsoft Community Hub](#)

Azure AD Graph API will be replaced by MS Graph API.

Resolution

AADS release 10.1.1.2 support MS Graph API.

Refer the below steps to make changes

Procedure

1. On Microsoft Azure, from App registration, navigate to your SSO application.
2. To grant consent on behalf of all users in your organization's directory, do the following:
 1. In Configured permissions, click Grant admin consent for <your admin name here> to grant consent on behalf of all users in your organization's directory.
 2. In the Confirmation window, enter your administrator credentials to confirm changes.
3. In the Manage section on the left-hand side of the screen, click API permissions.
4. Click Add a permission.
5. In the Request API permission section, click Microsoft Graph. Microsoft Graph displays the Permission Properties window.
6. Select Delegated permissions.
7. In the Select permissions area, click Directory and select the Directory.Read.All check box.
8. Click Add permissions.
9. Optional: If Microsoft Graph prompts you to enter your administrator credentials, repeat step 2.

Workaround or alternative remediation

Remarks

n/a

Patch Notes

Backup before applying the patch

n/a

Download

n/a

Patch install instructions

Service-interrupting?

n/a

n/a

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

n/a

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.