



KUARIO



All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Versie 1.0.6 geproduceerd op: November 2023 in Nieuw-Vennep.

Uitgever

KUARIO B.V.

Productie

KUARIO B.V.

Inhoudsopgave

Introduction

4

Configuration

5



Introduction

Admins can use their Single Sign On (SSO) configuration to enable and authorize the KUARIO integration for all users. End users will then be prompted to authorize this integration. To configure this integration, the account must have Single Sign-On configured and their identity provider must be federated with Azure Active Directory.

This setting has changed it is now disabled by default. It needs to be set to 'Yes' (enabled) to use KUARIO integrated with MS Office 365 / MS Active Directory within Azure.

Configuration

To enable end-user to use KUARIO as a federation of the MS Azure Active directory platform and authenticate with Office 365, one must first log in to KUARIO with the appropriate Microsoft account. Then Azure Active directory must be configured. To do this follow the next steps.

1. First use your KUARIO app or de site: '<https://login.kuario.com>' to login to KUARIO. Be sure to use the 'Sign in with Microsoft' option. As soon as you are logged in Azure's Active Directory should now have a KUARIO entry under Enterprise Applications.
2. In your Azure Dashboard go to 'Enterprise Applications ->Consent and permissions'.
3. Select 'Allow user consent for apps'.
4. Select 'Allow group owner consent for all group owners'.

[Home](#) > [Enterprise applications | Consent and permissions](#) >

Consent and permissions | User consent settings ...

Manage

 User consent settings

 Permission classifications



Save



Discard



Got feedback?

Control when end users and group owners are allowed to grant consent to applications, and when they will be required to request administrator review and approval. Allowing users to grant apps access to data helps them acquire useful applications and be productive, but can represent a risk in some situations if it's not monitored and controlled carefully.

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. [Learn more](#)

Do not allow user consent

An administrator will be required for all apps.

Allow user consent for apps from verified publishers, for selected permissions (Recommended)

All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

Allow user consent for apps

All users can consent for any app to access the organization's data.



With your current user settings, all users can allow applications to access your organization's data on their behalf. [Learn more about the risks](#)
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". [Learn more](#)

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. [Learn more](#)

Do not allow group owner consent

Group owners cannot allow applications to access data for the groups they own.

Allow group owner consent for selected group owners

Only selected group owners can allow applications to access data for the groups they own.

Allow group owner consent for all group owners

All group owners can allow applications to access data for the groups they own.

- Go to 'Enterprise Applications -> KUARIO -> Permissions'. Remember you have to have been signed in at least once using the Microsoft account belonging to this active directory.
- Grant admin consent for the enterprise (in this example 'inepro'), in your case this should be the name of your organization.

Dashboard > Enterprise applications > KUARIO

KUARIO | Permissions

Enterprise Application

Refresh Review permissions Got feedback?

Permissions

Applications can be granted permissions to your organization and its users by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more](#).
As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

Grant admin consent for [organization name]

Admin consent User consent

Search permissions

API Name	Permission	Type	Granted through	Granted by
Microsoft Graph				
Microsoft Graph	Sign in and read user profile	Delegated	Admin consent	An administrator
Microsoft Graph	Read and write files in all site collections	Application	Admin consent	An administrator
Microsoft Graph	Read files in all site collections	Application	Admin consent	An administrator

- Your users should now be able to use single sign on with their Microsoft Azure Active directory / Microsoft Office 365 account for KUARIO (again).

