SHAREPOINT JUST-IN-TIME (JIT) PERMISSIONS DOCUMENTATION Mysolution

Microsoft Business Central

Support - Support@mysolution.nl

Contents

1.   Introduction

This documentation is for version 23.01.00 or higher, provided Graph authentication and application permissions are used.

1.1.   Advantages of Just-In-Time (JIT) Permissions

The main advantages are:
- Grants users the required permissions on SharePoint at when necessary.
  Users no longer need permissions on SharePoint.
- Permissions can automatically be revoked (via JobQueue).
  This process only revokes a permission that was added with this functionality, for a specific user, on a specific item (file). Permissions granted via SharePoint remain intact.
  Therefore it is still possible to setup permissions on the site/drive or folder level.

1.2.   Requirements

The following requirements need to be met in order for JIT to work properly.
- Users must log into Business Central using Single Sign-On (SSO)
- Users need to have an Microsoft 365 Authentication Email set on the user card.

Microsoft 365

Authentication Email · · · · · [   ]

- The same emailaddress needs to be known in AAD. It is on this emailaddress that permissions are granted on SharePoint.
- Use of Application Permissions
- Using JIT in combination with 'Open Office files in: Desktop App' does not work and is therefore not available at the same time.

Open Office files in · · · · · · · · · · · · · · · [Desktop App   ∨]

- A JobQueue needs to be run periodically to automatically revoke granted permissions, otherwise granted permissions will remain and grow over time (this can be automatically done during setup, more on this later).
- As always, SharePoint (and the JobQueue) need to be set per company.

2. Setup

New groups and buttons are available on the SharePoint Setup (Mysolution) page.

Security

Use JIT Permissions · · · · · · · · · ·	⬤ (off)
Revoke JIT Permissions · · · · · · · ·	⬤ (off)
JIT Permissions Lifetime (in hours) · · ·	12
Open Read-only files in mode · · · · · ·	Download

- **Use JIT Permissions**
  Enables the creation of JIT permissions when opening files.

- **Revoke JIT Permissions**
  Enables automatically revoking JIT permissions (via JobQueue).

- **JIT Permissions Lifetime (in hours)**
  The lifetime that permissions will remain active.

- **Open Read-only files in mode** (Download, Online)
  Download is the 'old' behaviour, Online is the new option where for instance read-only files can be opened in the browser.

SharePoint Action JobQueue

Status ·	
Earliest Start Date/Time · · · · · · · · · ·	

This shows details about the SharePoint Action JobQueue (if it exists).

📷 Test Connection   🌐 Token Cache Overview   📑 View Action Queue   📑 View JobQueue Entry

The buttons become available when either '**Revoke JIT Permissions**' or '**Queue items for deletion**' are enabled.
Both of those settings will create SharePoint Actions which require a JobQueue to process.
Clicking the 'View JobQueue Entry' opens that JobQueue (will be created first if it does not exist).
The 'View Action Queue' opens all pending actions or errors.

The required JobQueue can be automatically created by clicking the 'View JobQueue Entry' button.
The user will also be prompted to create it when enabling options that require it.

> (?) No JobQueue found for "MYS SharePoint Action JQ" (11096168),
> which is required for (Queue Files For Deletion, Revoke JIT Permissions).
> Do you want to setup the JobQueue Entry now?
>
> [Yes]   [No]

2.1. 'Request Access' and 'Access Denied' pages

When a user no longer has access to a given item, they will be confronted with a 'Request Access' page or a 'Access Denied' page (depending on how SharePoint is setup).
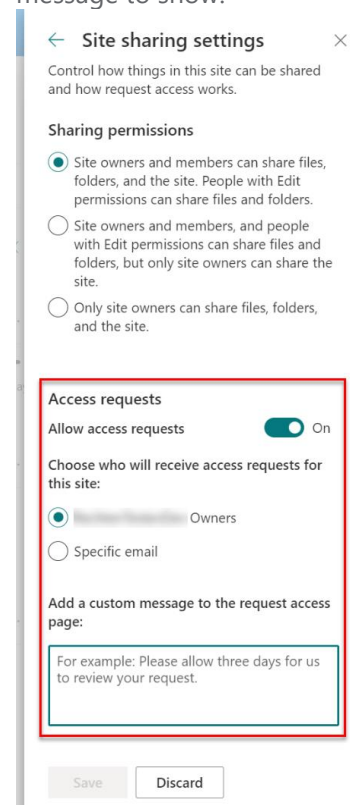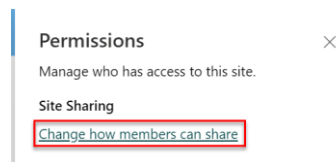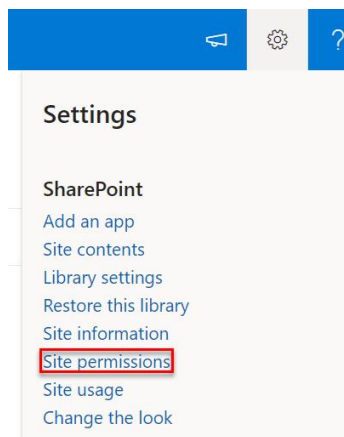
For example, a user opens a document on SharePoint on Tuesday, and refreshes that page on Wednesday. The permission has been revoked in the meantime.

To resolve this, the user simply has to re-open the file in Business Central, see also 3.1.
The page that the user sees is somewhat customizable.

2.1.1 Customizing the 'Request Access' or 'Access Denied' pages

Go to 'Settings', 'Site permissions'.   Click on 'Change how members can share'.   In the 'Access requests' block you can for instance setup what message to show.

For more information see:
https://support.microsoft.com/en-us/office/set-up-and-manage-access-requests-94b26e0b-2822-49d4-929a-8455698654b3
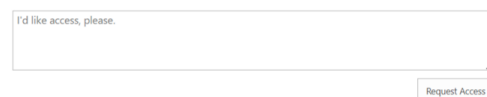
A custom message can be setup to be shown on the page.
A specific e-mail can also be set in case a user does end up 'requesting access'.

Disabling 'Allow access requests' is presumably the preferred option.

Page 'Access Denied'
'Allow access requests' is disabled
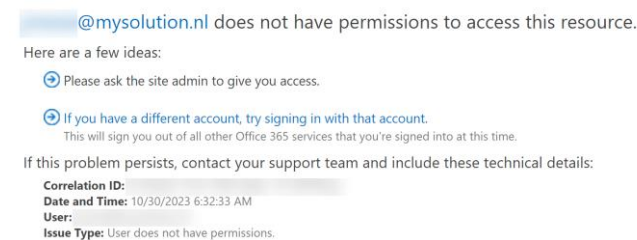
Page 'Request Access'
'Allow access requests' is enabled

3.   Troubleshooting

Consult the manual 'Mysolution - Troubleshooting Graph' if the problem is not described here.

3.1.   You need permission to access this item

You need permission to access this item.

I'd like access, please.

Request Access

Solution:
- The user has to open the interaction again via Business Central.

3.2.   'Access Denied'

Access Denied

@mysolution.nl does not have permissions to access this resource.

Here are a few ideas:

Please ask the site admin to give you access.

If you have a different account, try signing in with that account.
This will sign you out of all other Office 365 services that you're signed into at this time.

If this problem persists, contact your support team and include these technical details:

Correlation ID:
Date and Time: 10/30/2023 6:32:33 AM
User:
Issue Type: User does not have permissions.

Solution:
- The user has to open the interaction again via Business Central.