What is this Modern Authentication everyone is talking about, and why you should phase out Legacy authentication?

By Erik Loef & Kenneth van Surksum

About://us

ERIK LOEF

- CTO at Proxsys
- Microsoft MVP – Cloud & Datacenter Management
- Board member of the WPNinjasNL

- Blog: https://www.proxsys.nl/actueel/blog/
- Twitter: @erikloef

KENNETH VAN SURKSUM

- Modern Workplace Consultant at Insight24
- Co-founder and board member of the WPNinjasNL

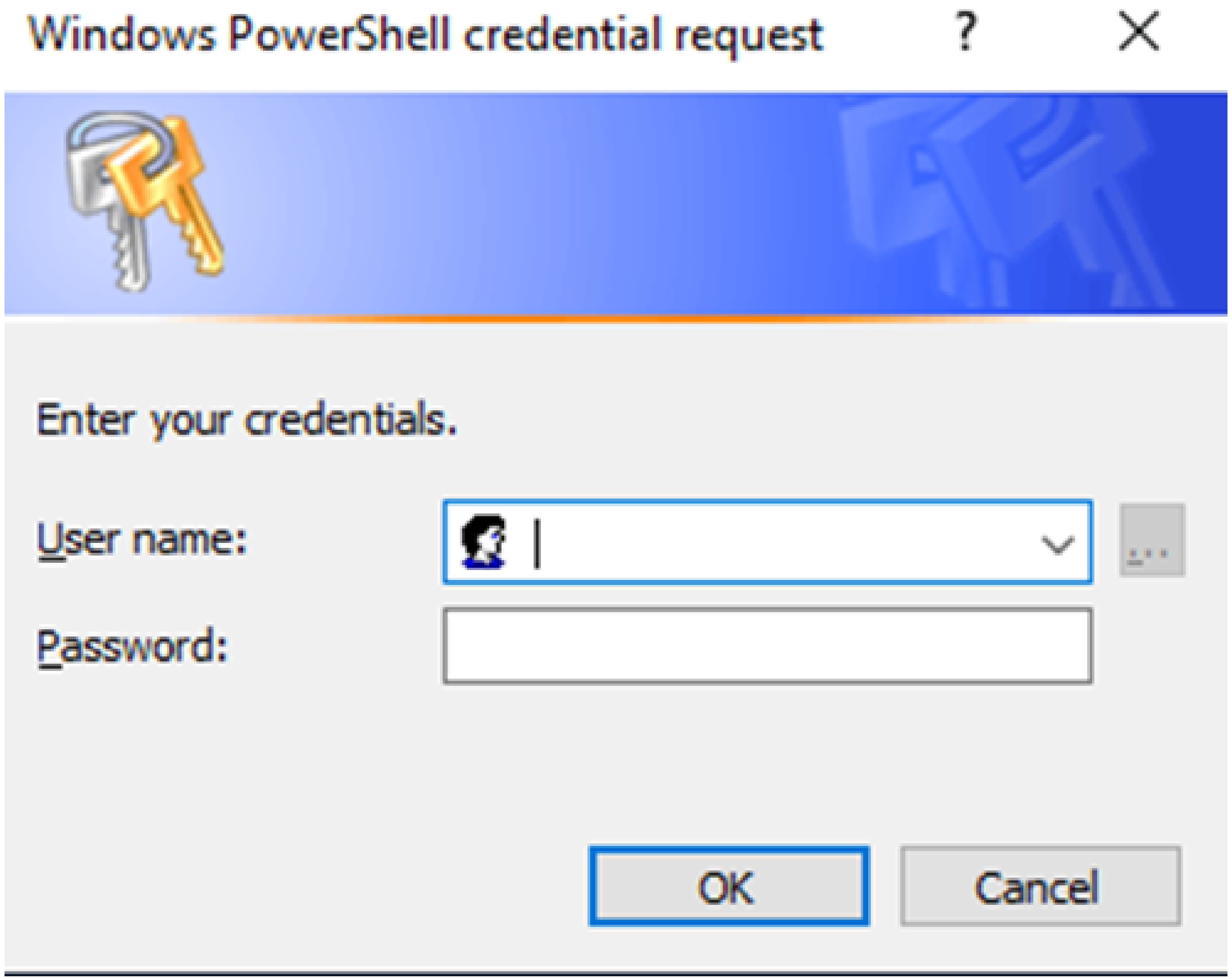
- Blog: https://vansurksum.com
- Twitter: @kennethvs

Agenda

1. What is legacy authentication?
2. What is modern authentication?
3. How to detect legacy authentication?
4. Steps to migrate from legacy to modern authentication?
5. Application consent
6. Call 2 Action

What is legacy authentication?

When using Basic/Legacy Authentication application sends a username and password with every request to f.e. Exchange Online which either forwards the credentials towards Azure AD or a federated authentication provider like Active Directory Federation Services (ADFS).



Windows PowerShell credential request

Enter your credentials.

User name:

Password:

What is the issue with legacy authentication?

The problem with Basic/Legacy authentication is that it is vulnerable to brute force or password spray attacks.

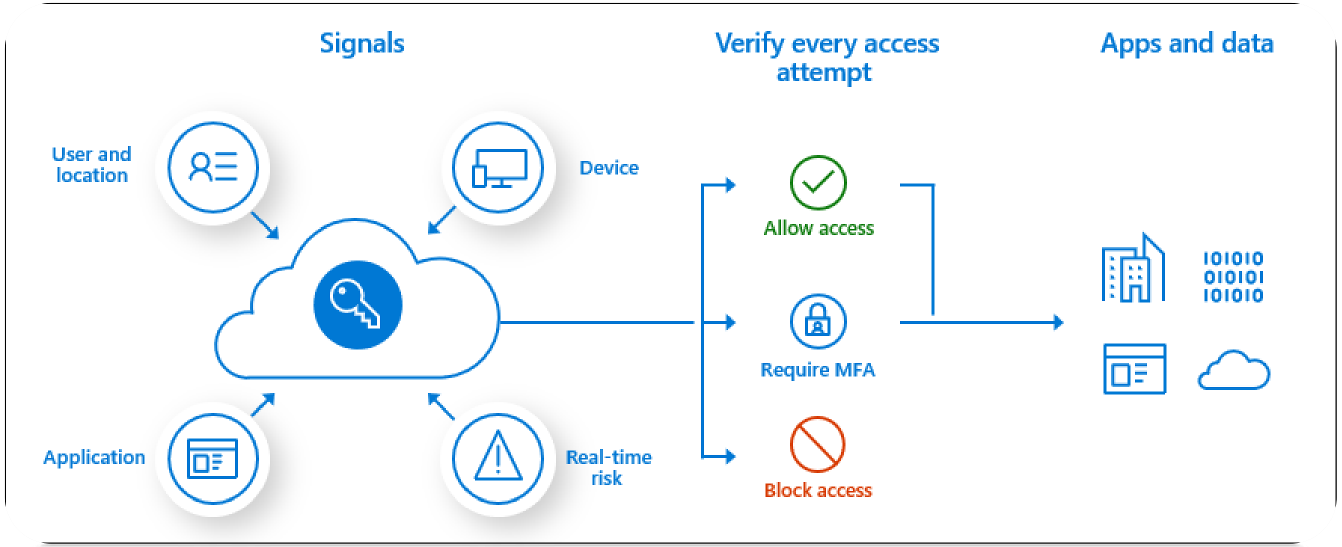
And therefore:

~~Microsoft announced that it will disable legacy authentication in the second half of 2021*~~

*Initially they announced it to be disabled on October 13, 2020 but due to the COVID-19 crisis Microsoft decided to postpone until further notice

Some additional reasons

- In order to fully implement Conditional Access we must make sure that the services that we want to protect using Conditional Access make use of Modern Authentication
- If we want to move towards Passwordless we must stop using Legacy Authentication



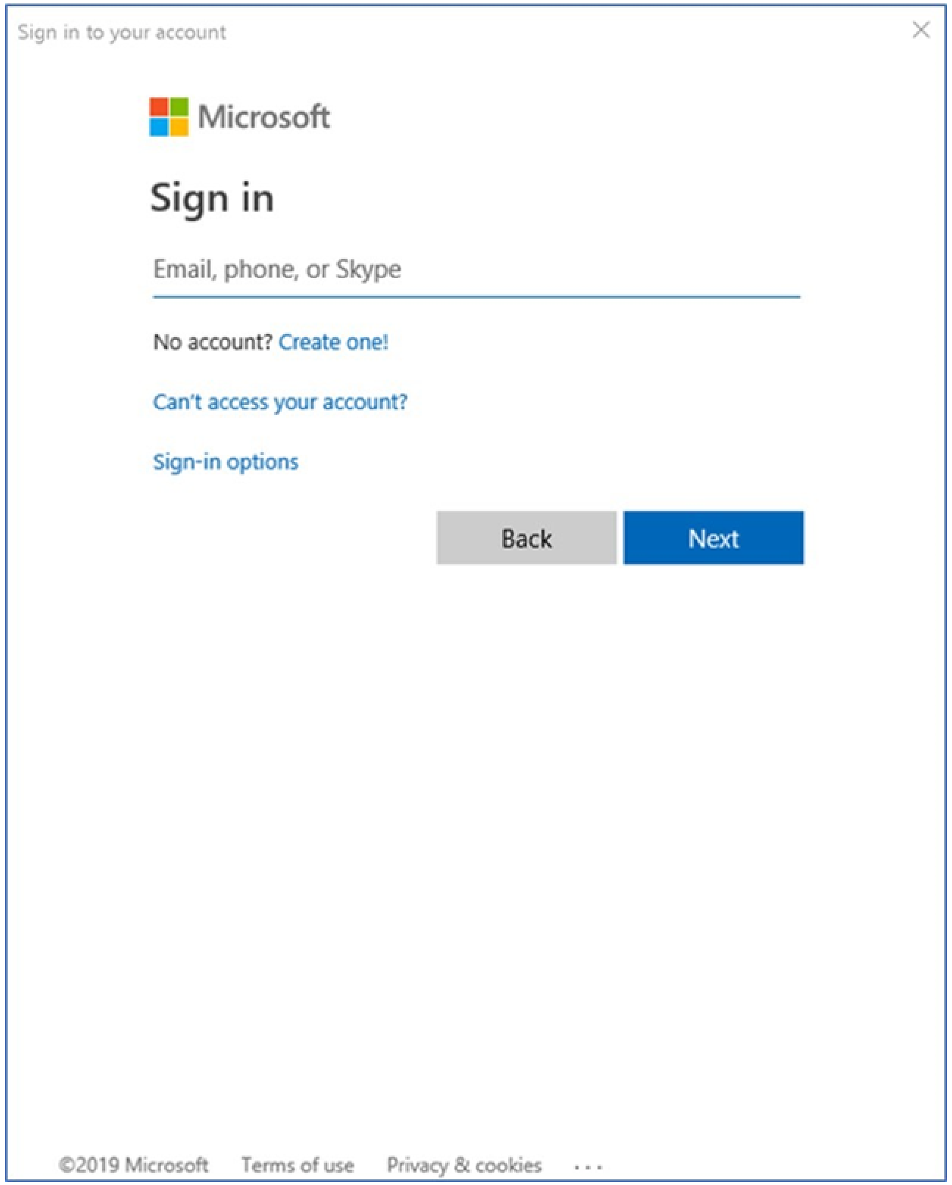
Bypassing MFA through CA by using Legacy authentication

So, what is Modern authentication

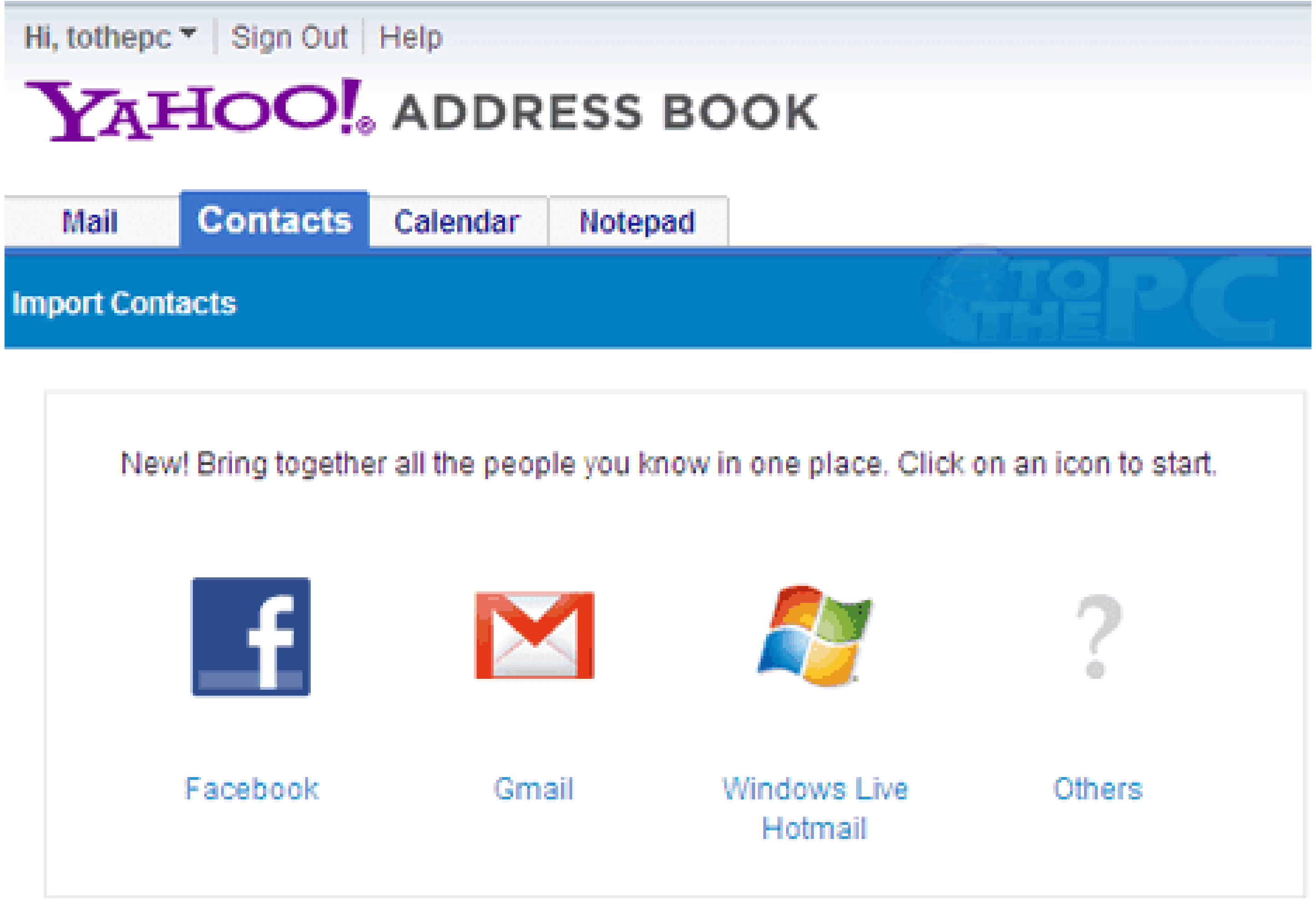
Modern Authentication is based on OAuth 2.0 and the Active Directory Authentication Library (ADAL) providing **token-based authentication**. OAuth 2.0 in this case is the protocol being used, and ADAL is used to authenticate against Azure AD.

Token based authentication, as described by the World Wide Web Consortium (W3C):

“The general concept behind a token-based authentication system is simple. Allow users to enter their username and password in order to obtain a token which allows them to fetch a specific resource – without using their username and password. Once their token has been obtained, the user can offer the token – which offers access to a specific resource for a time period – to the remote site. Using some form of authentication: a header, GET or POST request, or a cookie of some kind, the site can then determine what level of access the request in question should be afforded. “



Before … OAUTH2.0


Hi, tothepc ▾ | Sign Out | Help

Import Contacts

New! Bring together all the people you know in one place. Click on an icon to start.

www.yahoo.com

get contacts from microsoft

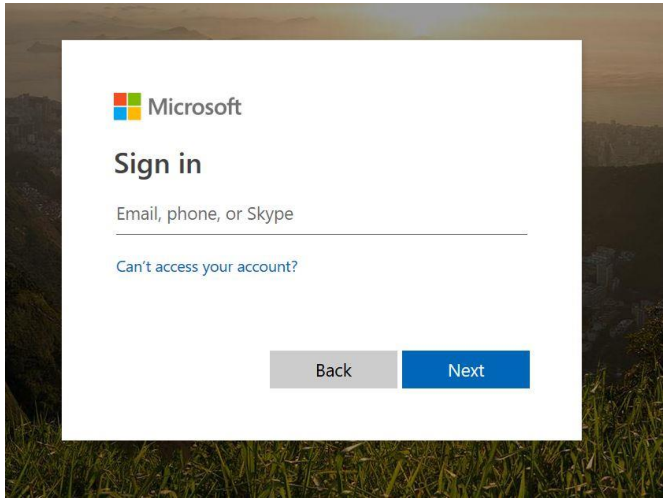
0

Resource owner

Go to authorisation server

Redirect URI
www.yahoo.com/callback
Response: code

login.microsoft.com



Microsoft

Sign in

Email, phone, or Skype

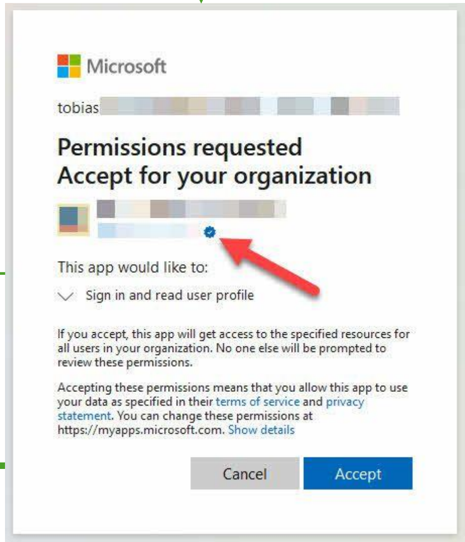
Can't access your account?

Back Next

Microsoft | Microsoft Graph

Get access token for auth. code

Access token



Microsoft

tobias[redacted]

Permissions requested
Accept for your organization

[redacted]

This app would like to:

Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Cancel Accept

Redirect URI
www.yahoo.com/callback

With authorisation code

www.yahoo.com/callback

OPENID CONNECT

- OAUTH = authorization
- OPENID CONNECT = authentication

- Adds an ID Token
- UserInfo Endpoint
- Standard scopes

OPENID Connect

www.yahoo.com

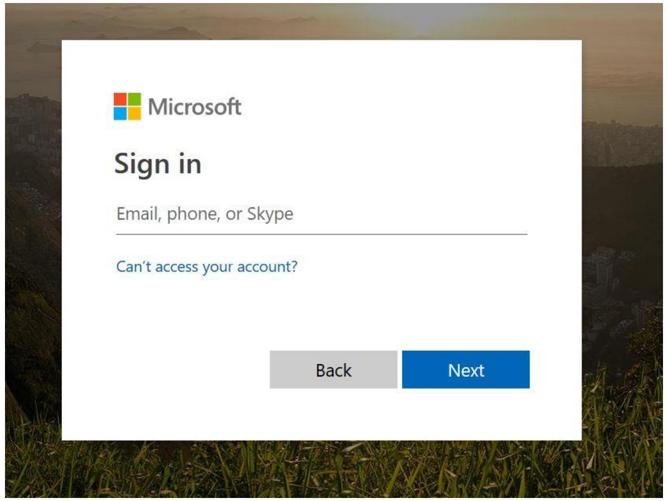
Get contacts from Microsoft

Resource owner

Go to authorisation server

Redirect URI
www.yahoo.com/callback
Response: code
Scope: openid

login.microsoft.com



Microsoft

Sign in

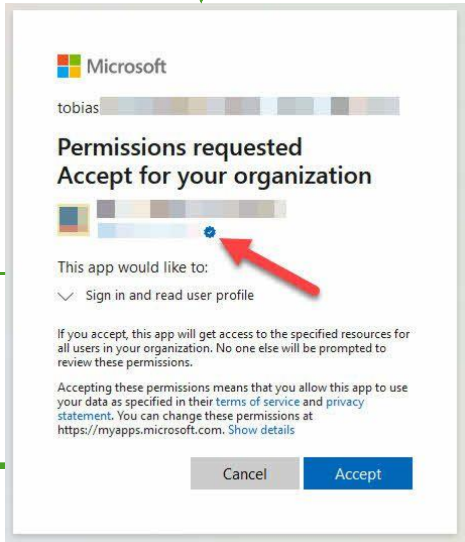
Email, phone, or Skype

Can't access your account?

Get access token for auth. code

Microsoft | Microsoft Graph

Access token



Microsoft

tobias [redacted]

Permissions requested
Accept for your organization

[redacted]

This app would like to:

Sign in and read user profile

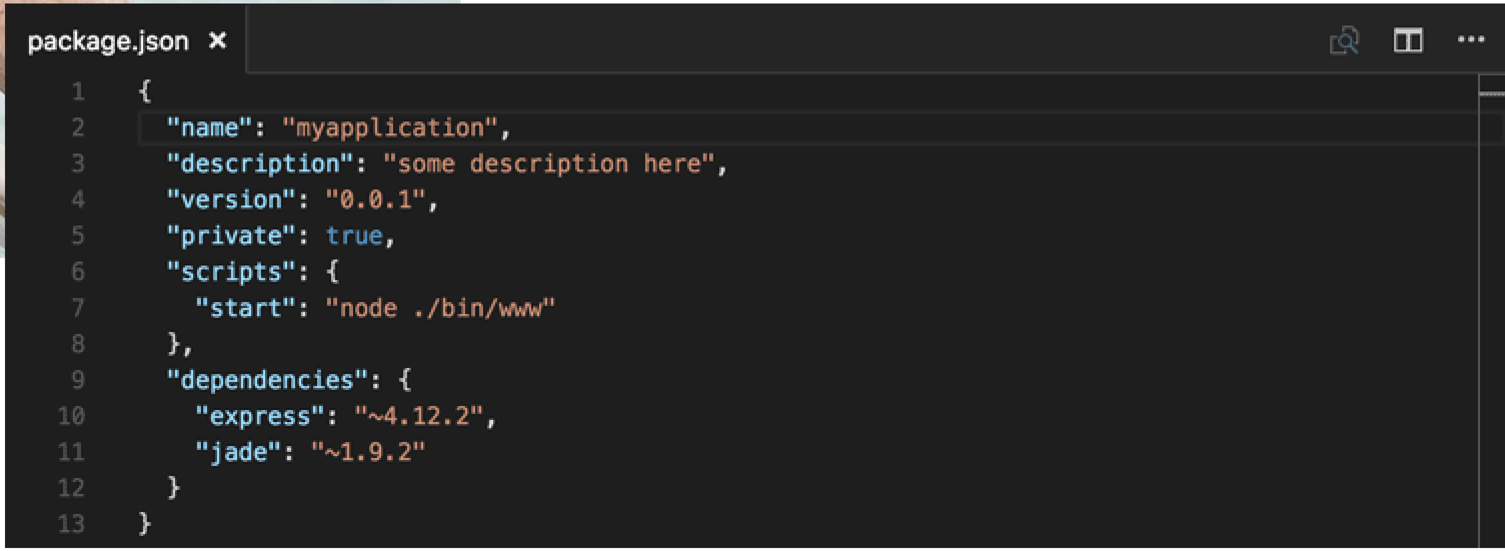
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Redirect URI
www.yahoo.com/callback

With authorisation code
userID token

www.yahoo.com/callback



```json
{
  "name": "myapplication",
  "description": "some description here",
  "version": "0.0.1",
  "private": true,
  "scripts": {
    "start": "node ./bin/www"
  },
  "dependencies": {
    "express": "~4.12.2",
    "jade": "~1.9.2"
  }
}
```

Modern Authentication

Why Modern Authentication?

Microsoft wants you to move towards Modern Authentication since it’s a ***more secure*** *solution. Another big advantage of using Modern Authentication is that it can leverage Azure AD Conditional Access, giving you the option to force MFA for users among other options.*

Determine whether legacy authentication is used by examining the Azure AD sign-in Logging and Workbooks

From Legacy -> Modern (1)

- 1. Enable Modern Authentication in Exchange Online and SharePoint Online
- 2. Create Conditional Access policy to block legacy authentication
- 3. Finished

From Legacy -> Modern (2)

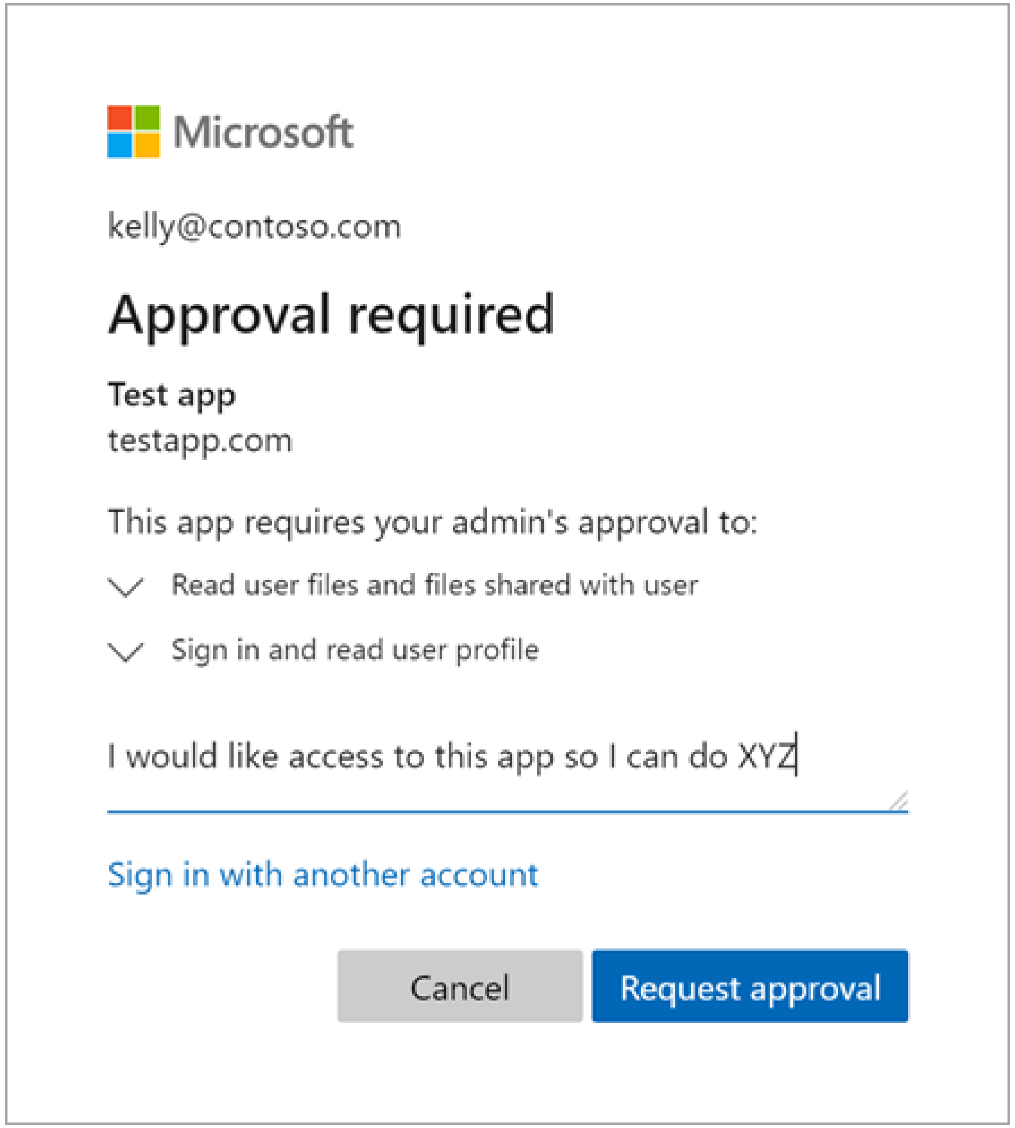
- 1. Enable Modern Authentication
- 2. Disable mailbox protocols which you do not want to be used
- 3. Create authentication policies disabling legacy authentication for the protocols you want to allow
- 4. Create supporting Conditional Access policies
- 5. Migrate your users one by one
  - From built in mail apps to Modern authentication apps

or

  - To Outlook (allowing you to also apply MAM)

Transition to Modern Authentication

Consent Risks



Microsoft

kelly@contoso.com

Approval required

Test app

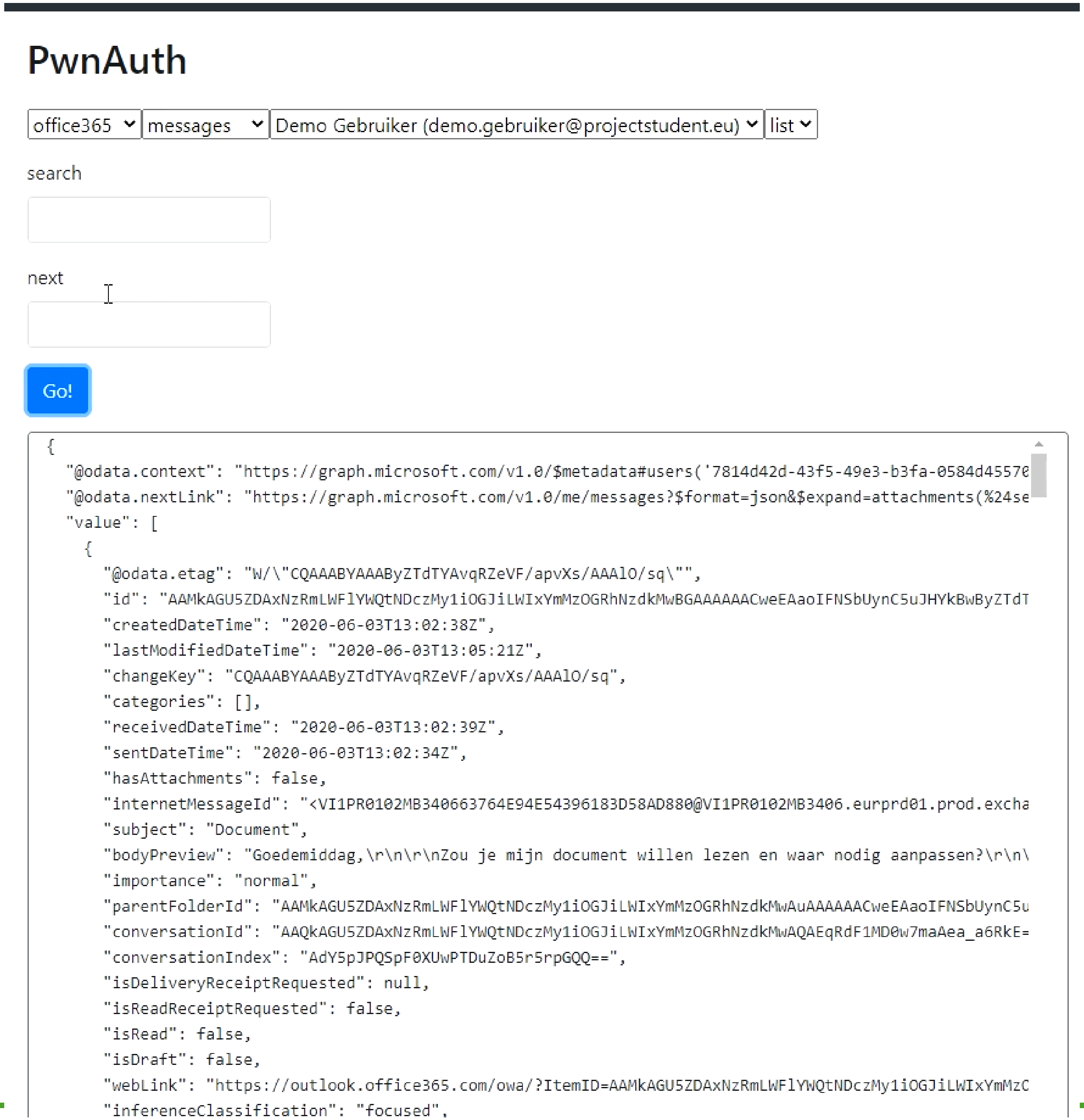
testapp.com

This app requires your admin's approval to:

- Read user files and files shared with user
- Sign in and read user profile

I would like access to this app so I can do XYZ

Consent Risks



PwnAuth

office365 | messages | Demo Gebruiker (demo.gebruiker@projectstudent.eu) | list

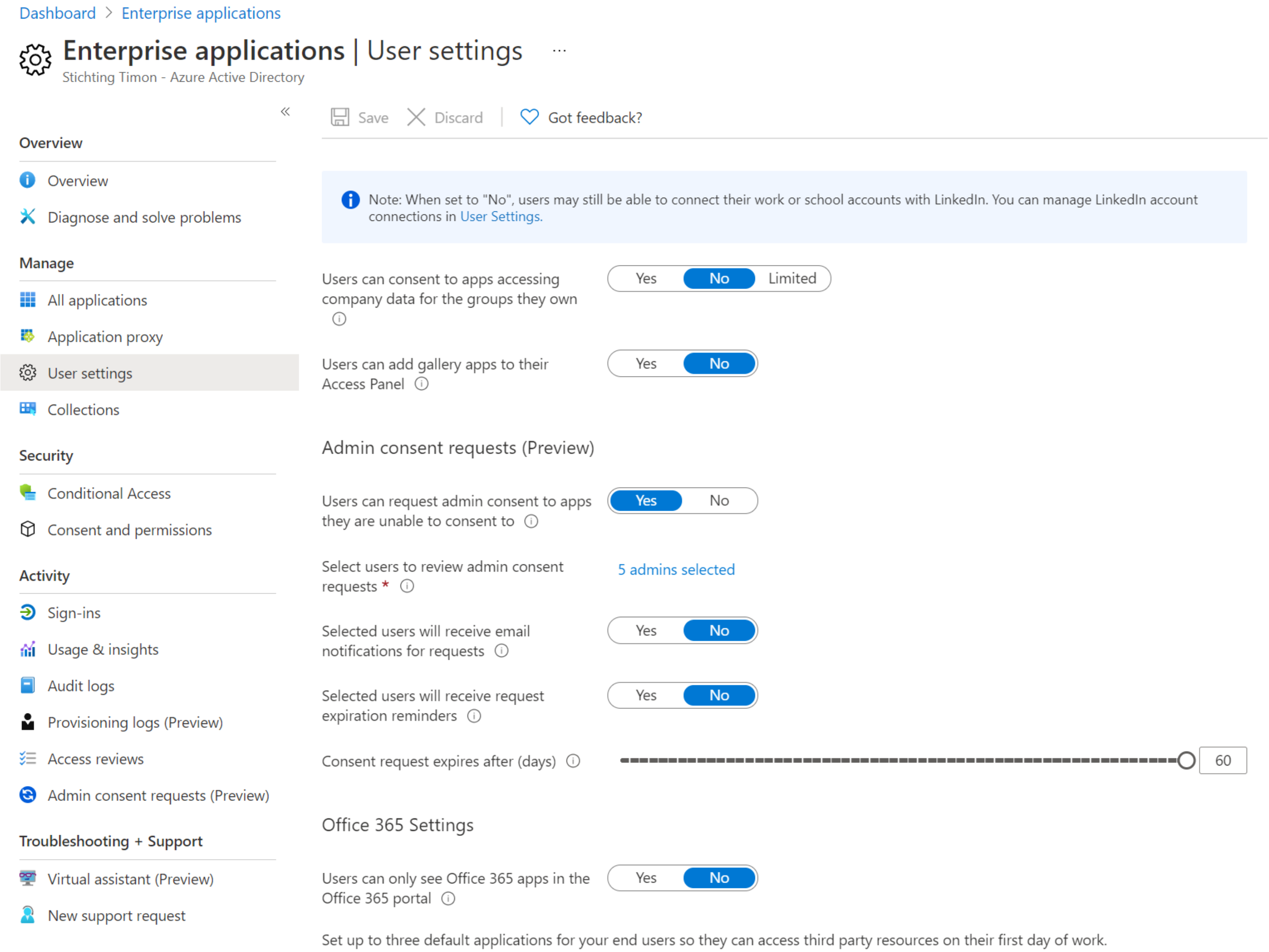
search

next

```
{
  "@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users('7814d42d-43f5-49e3-b3fa-0584d4557
  "@odata.nextLink": "https://graph.microsoft.com/v1.0/me/messages?$format=json&$expand=attachments(%24se
  "value": [
    {
      "@odata.etag": "W/\"CQAAABYAAAByZTdTYAvqRZeVF/apvXs/AAAlO/sq\"",
      "id": "AAMkAGU5ZDAxNzRmLWFlYWQtNDczMy1iOGJiLWIxYmMzOGRhNzdkMwBGAAAAAACweEAaoIFNSbUynC5uJHYkBwByZTdT
      "createdDateTime": "2020-06-03T13:02:38Z",
      "lastModifiedDateTime": "2020-06-03T13:05:21Z",
      "changeKey": "CQAAABYAAAByZTdTYAvqRZeVF/apvXs/AAAlO/sq",
      "categories": [],
      "receivedDateTime": "2020-06-03T13:02:39Z",
      "sentDateTime": "2020-06-03T13:02:34Z",
      "hasAttachments": false,
      "internetMessageId": "<VI1PR0102MB340663764E94E54396183D58AD880@VI1PR0102MB3406.eurprd01.prod.excha
      "subject": "Document",
      "bodyPreview": "Goedemiddag,\r\n\r\nZou je mijn document willen lezen en waar nodig aanpassen?\r\n\
      "importance": "normal",
      "parentFolderId": "AAMkAGU5ZDAxNzRmLWFlYWQtNDczMy1iOGJiLWIxYmMzOGRhNzdkMwAuAAAAAACweEAaoIFNSbUynC5u
      "conversationId": "AAQkAGU5ZDAxNzRmLWFlYWQtNDczMy1iOGJiLWIxYmMzOGRhNzdkMwAQAEqRdF1MD0w7maAea_a6RkE=
      "conversationIndex": "AdY5pJPQSpF0XUwPTDuZoB5r5rpGQQ==",
      "isDeliveryReceiptRequested": null,
      "isReadReceiptRequested": false,
      "isRead": false,
      "isDraft": false,
      "webLink": "https://outlook.office365.com/owa/?ItemID=AAMkAGU5ZDAxNzRmLWFlYWQtNDczMy1iOGJiLWIxYmMzC
      "inferenceClassification": "focused",
```

Consent Risks

How to prevent and investigate ?



Enterprise applications | User settings ...

Stichting Timon - Azure Active Directory

Note: When set to "No", users may still be able to connect their work or school accounts with LinkedIn. You can manage LinkedIn account connections in User Settings.

Users can consent to apps accessing company data for the groups they own ⓘ — Yes [✓ No] Limited

Users can add gallery apps to their Access Panel ⓘ — Yes [✓ No]

Admin consent requests (Preview)

Users can request admin consent to apps they are unable to consent to ⓘ — [✓ Yes] No

Select users to review admin consent requests * ⓘ — 5 admins selected

Selected users will receive email notifications for requests ⓘ — Yes [✓ No]

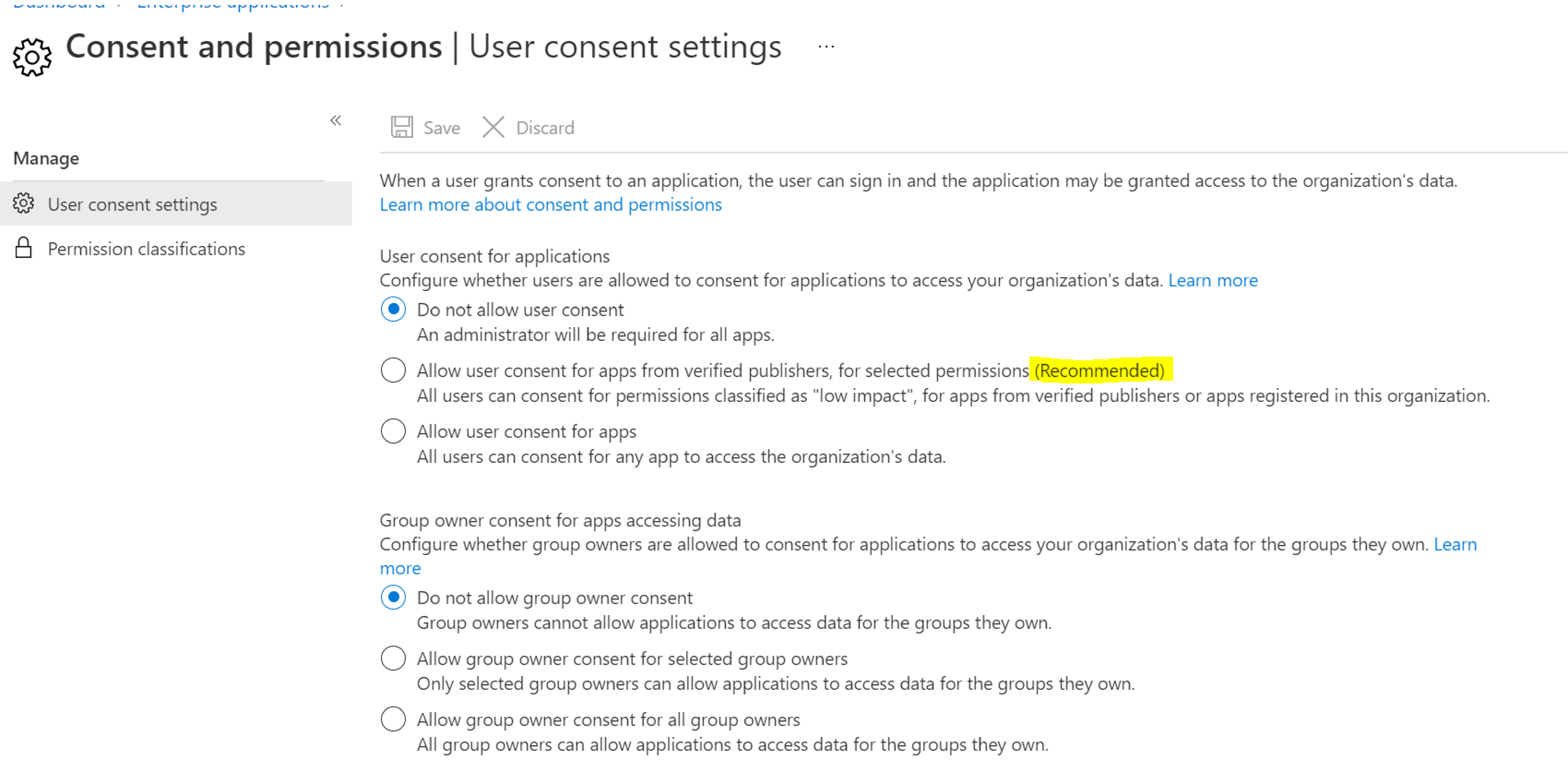
Selected users will receive request expiration reminders ⓘ — Yes [✓ No]

Consent request expires after (days) ⓘ — 60

Office 365 Settings

Users can only see Office 365 apps in the Office 365 portal ⓘ — Yes [✓ No]

Set up to three default applications for your end users so they can access third party resources on their first day of work.



Dashboard > Enterprise applications >

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

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.

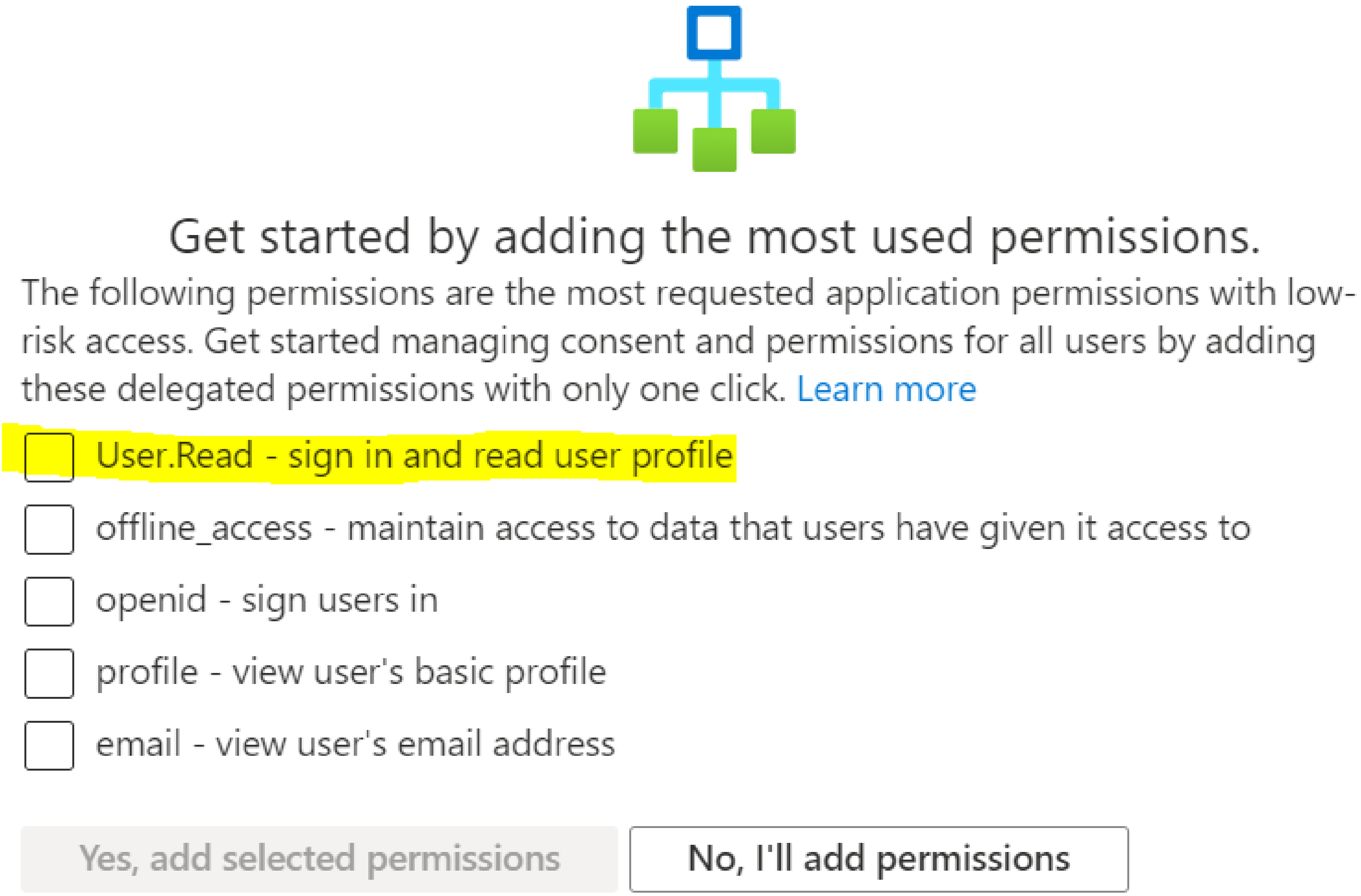
○ Allow user consent for apps
All users can consent for any app to access the organization's data.

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.



Get started by adding the most used permissions.

The following permissions are the most requested application permissions with low-risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. Learn more

□ User.Read - sign in and read user profile

□ offline_access - maintain access to data that users have given it access to

□ openid - sign users in

□ profile - view user's basic profile

□ email - view user's email address

Investigate the current situation

Illicit Grant blog by Microsoft
Detect and Remediate Illicit Consent Grants - Office 365 | Microsoft Docs

Get-AzureADPSPermissions.ps1
https://gist.github.com/psignoret/41793f8c6211d2df5051d77ca3728c09

TAKEAWAY

Make yourself ready for the next security steps

- Disable Basic Authentication
- Enforce MFA
- Govern your Consent

- Follow the Microsoft 30-60-90 guide

  https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/security-roadmap?view=o365-worldwide

Call 2 action

- Block Legacy Authentication
- If not possible
  - analyze basic authentication logons
  - make exceptions for only those logons
  - Add IP location for example
- Understand OAUTH2.0
  it is the new NTLM / Kerberos!
- Enable MFA
- Federate applications to Azure AD
- Govern the consents of Applications in your organization