# Azure AD, Graph and Exchange Online: A powerful combination

Ingo Gegenwarth

THE BEST RUN SAP

# Agenda

- Tenant-wide configuration
  - Illicit Consent Grants
  - Configure how end-users consent to applications
  - Conditional Access/MCAS
  - …

- Service Principal/Application configuration

- Exchange Online:
  - EWS/REST protocol
  - Client Access Rule

- Access token and recipient permissions:
  - How to request an access token
  - I now have an access token. Now I’m good to go?

- Real-life examples

# About me

Ingo Gegenwarth

IT Principal Consultant @SAP

MCM Exchange 2010

Office Server and Services MVP

Blog:

https://ingogegenwarth.wordpress.com/

Twitter:

@IngoGegenwarth

E-mail:

ingo@thecluelessguy.de

# What is illicit consent?

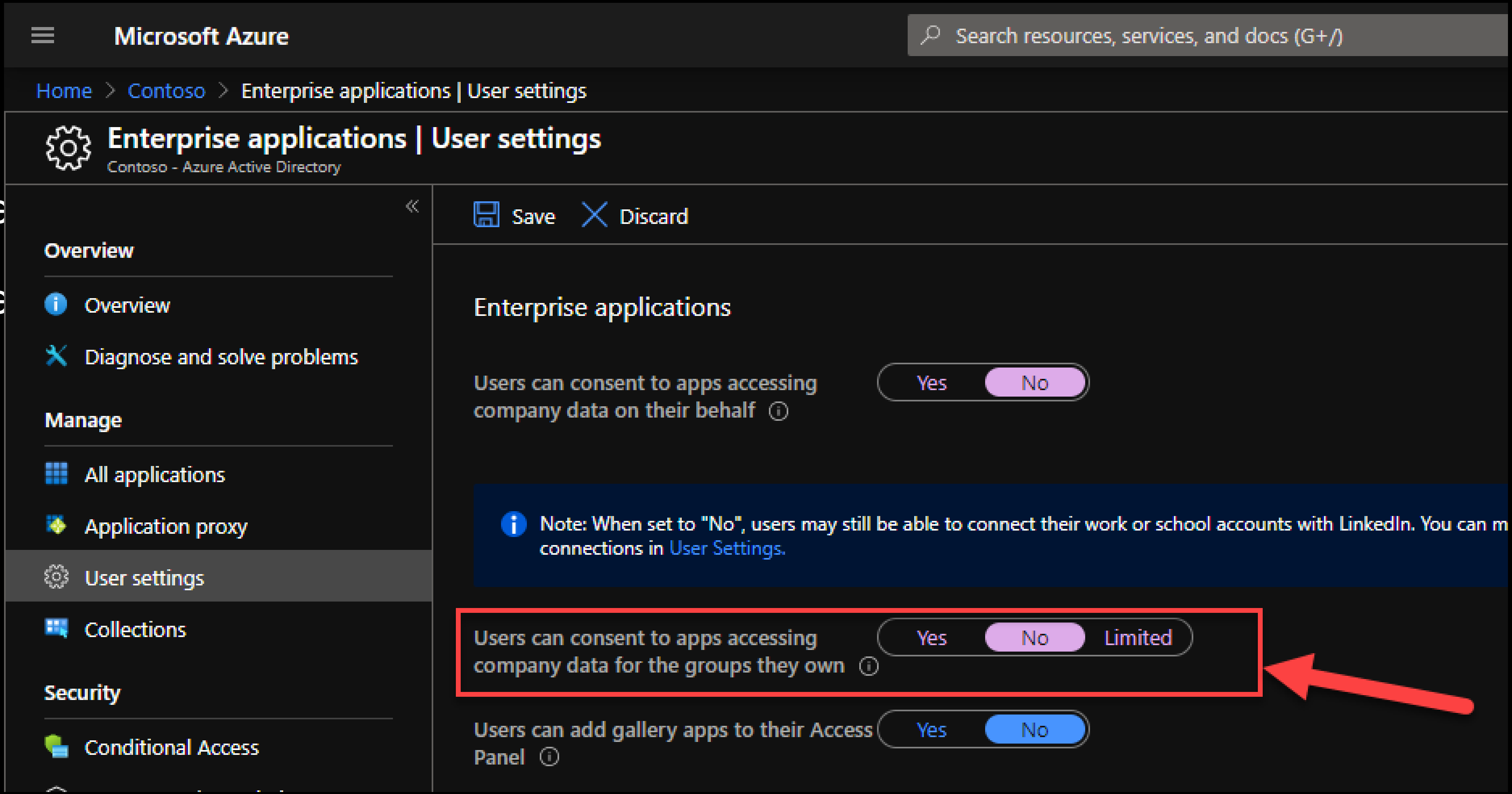
“In an illicit consent grant attack, the attacker creates an Azure-registered application that requests access to data such as contact information, email, or documents. The attacker then tricks an end user into granting that application consent to access their data either through a phishing attack, or by injecting illicit code into a trusted website. After the illicit application has been granted consent, it has account-level access to data without the need for an organizational account. Normal remediation steps, like resetting passwords for breached accounts or requiring Multi-Factor Authentication (MFA) on accounts, are not effective against this type of attack, since these are third-party applications and are external to the organization.”

**Credit: Microsoft**

# Tenant settings

Protecting

- Disable
- Disable



Home > Contoso > Enterprise applications | User settings

## Enterprise applications | User settings

Contoso - Azure Active Directory

Enterprise applications

Users can consent to apps accessing company data on their behalf ⓘ — Yes [✓ No]

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

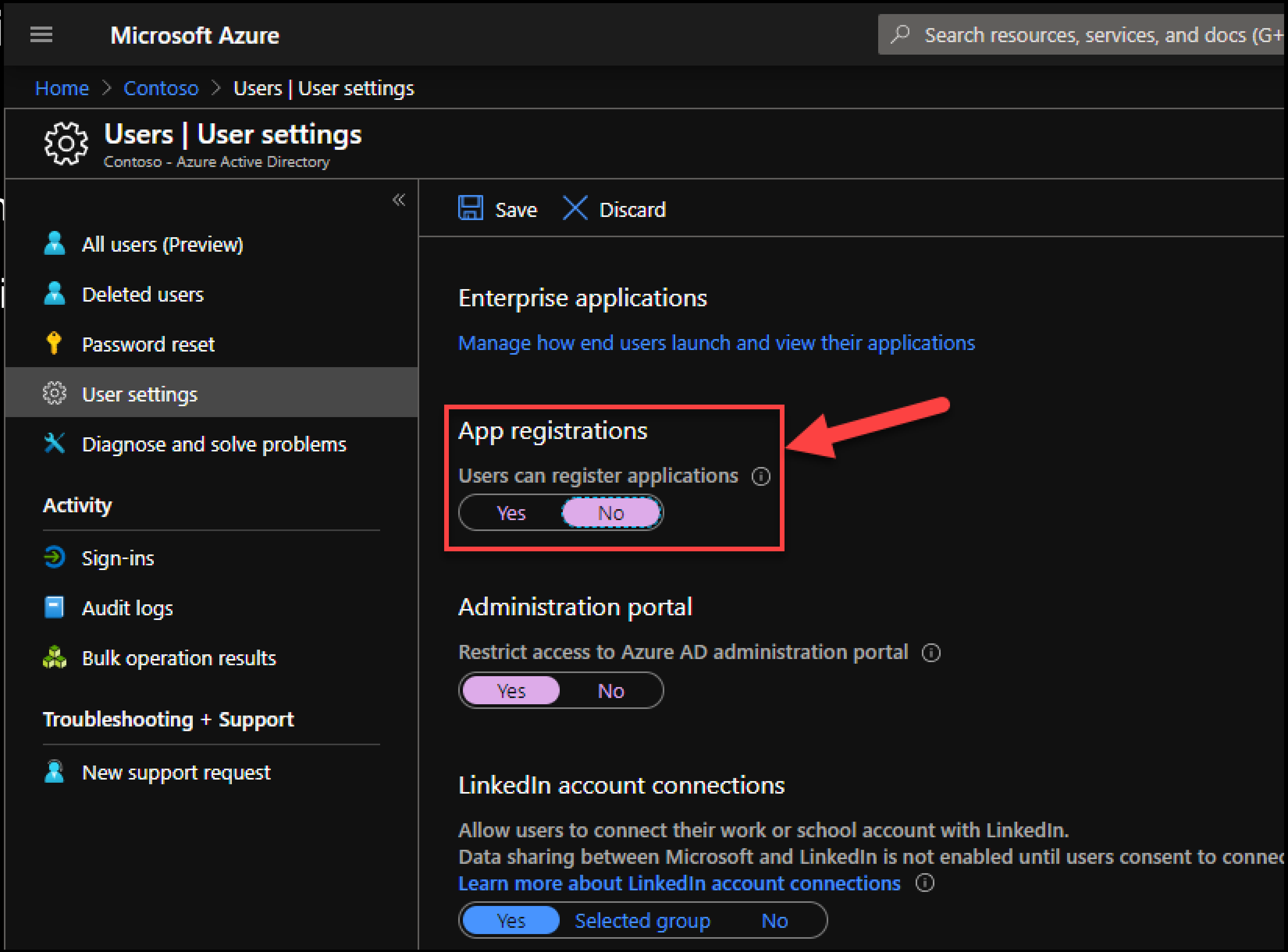
Users can consent to apps accessing company data for the groups they own ⓘ — Yes [✓ No] Limited

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

# Tenant setti

Configuration h

- Disable abili



Microsoft Azure
Search resources, services, and docs (G+
Home > Contoso > Users | User settings

## Users | User settings

Contoso - Azure Active Directory

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications: Yes [✓ No]

Administration portal

Restrict access to Azure AD administration portal: [✓ Yes] No

LinkedIn account connections

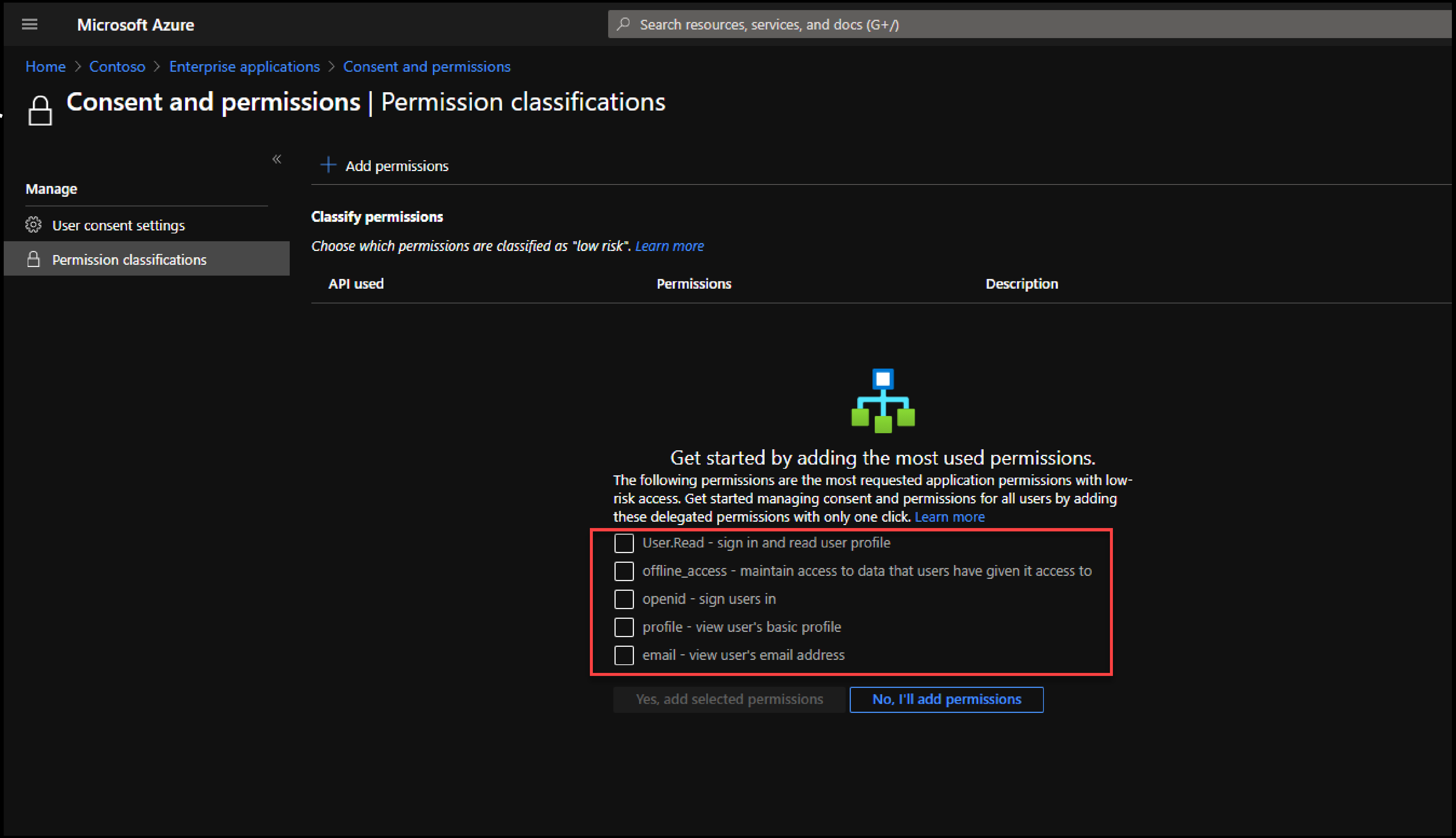
Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connec
Learn more about LinkedIn account connections

[✓ Yes] Selected group No

# Tenant settings

Configur

- Allow



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Contoso > Enterprise applications > Consent and permissions

## Consent and permissions | Permission classifications

+ Add permissions

Manage

User consent settings

Permission classifications

**Classify permissions**

*Choose which permissions are classified as "low risk". Learn more*

| API used | Permissions | Description |
|---|---|---|

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

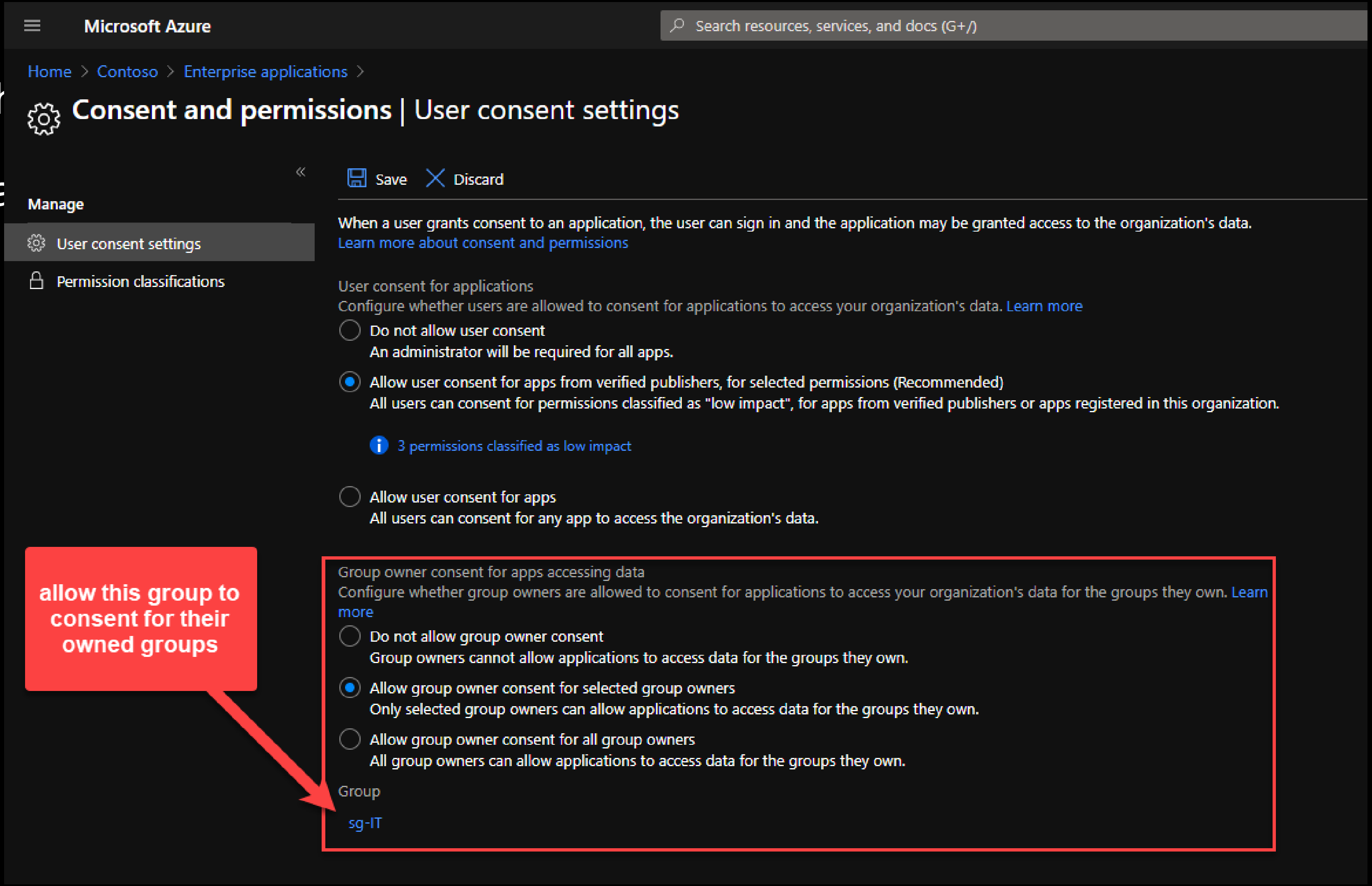
- □ User.Read - sign in and read user profile
- □ offline_access - maintain access to data that users have given it access to
- □ openid - sign users in
- □ profile - view user's basic profile
- □ email - view user's email address

Yes, add selected permissions | No, I'll add permissions

# Tenant settings

Configuration h

- Allow only a



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Contoso > Enterprise applications >

## Consent and permissions | User consent settings

Manage
User consent settings
Permission classifications
Save
Discard

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.

3 permissions classified as low impact

○ 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.

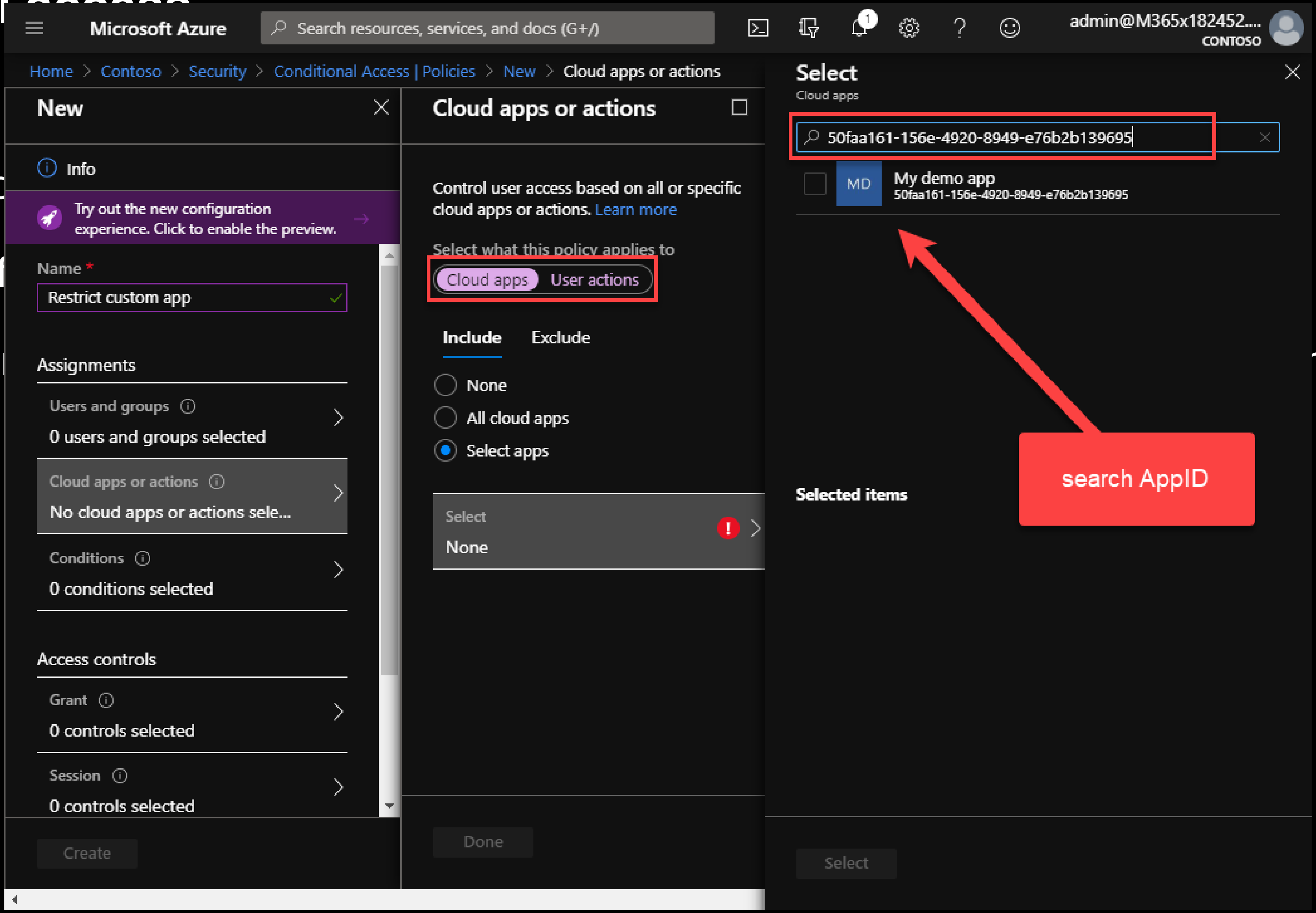
Group
sg-IT

allow this group to consent for their owned groups

# Conditional access

- By default c
- Best way of

Note: Conditio ... nissions!



Home > Contoso > Security > Conditional Access | Policies > New > Cloud apps or actions

**New**

Info

Try out the new configuration experience. Click to enable the preview.

Name *: Restrict custom app

Assignments

Users and groups: 0 users and groups selected

Cloud apps or actions: No cloud apps or actions sele...

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Create

**Cloud apps or actions**

Control user access based on all or specific cloud apps or actions. Learn more

Select what this policy applies to: Cloud apps | User actions

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Done

**Select**
Cloud apps

50faa161-156e-4920-8949-e76b2b139695

□ MD My demo app
50faa161-156e-4920-8949-e76b2b139695

Selected items

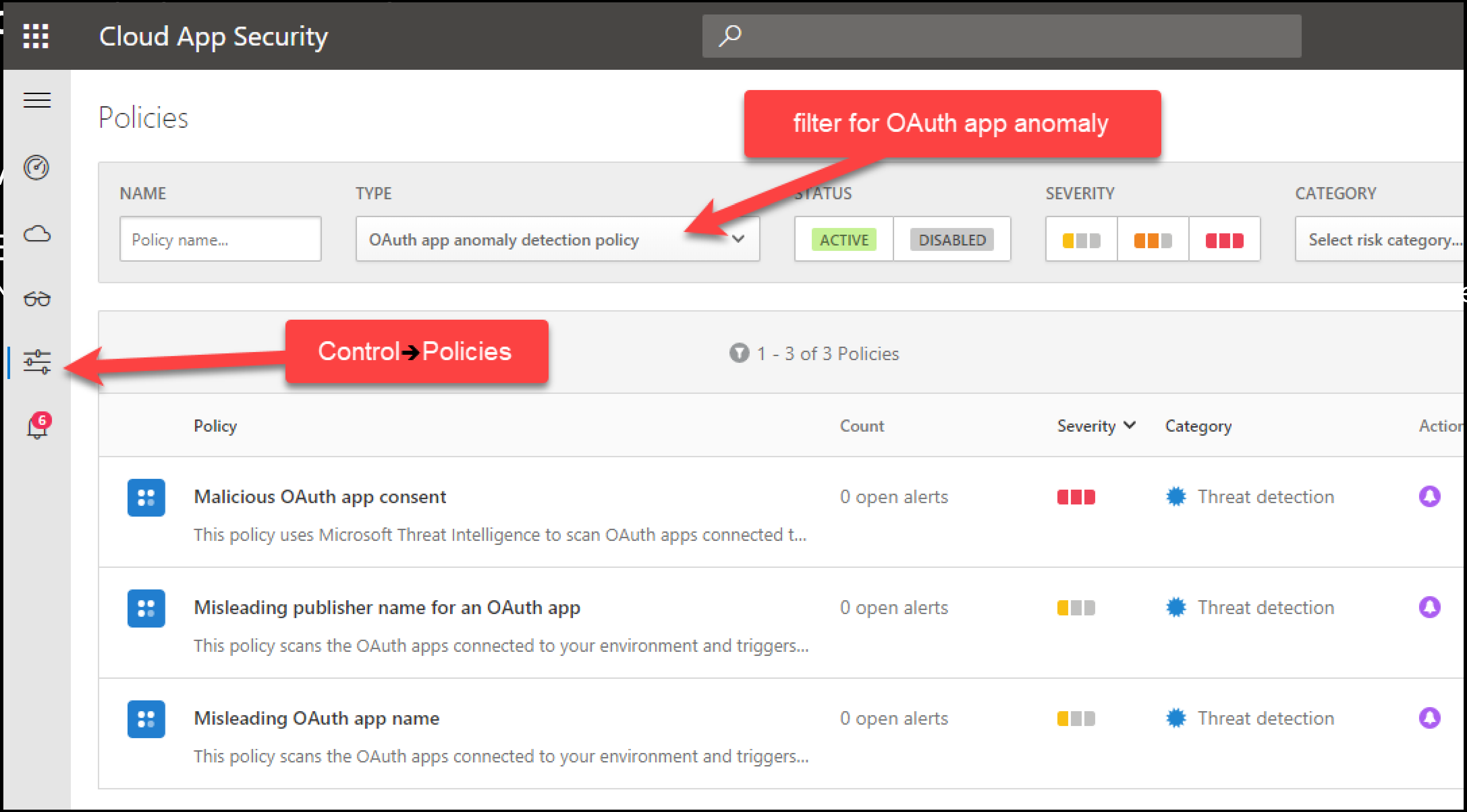
search AppID

Select

# Mic

MC

- E
  N eds.



Cloud App Security

Policies

filter for OAuth app anomaly

| NAME | TYPE | STATUS | SEVERITY | CATEGORY |
|---|---|---|---|---|
| Policy name... | OAuth app anomaly detection policy | ACTIVE DISABLED | | Select risk category... |

Control→Policies

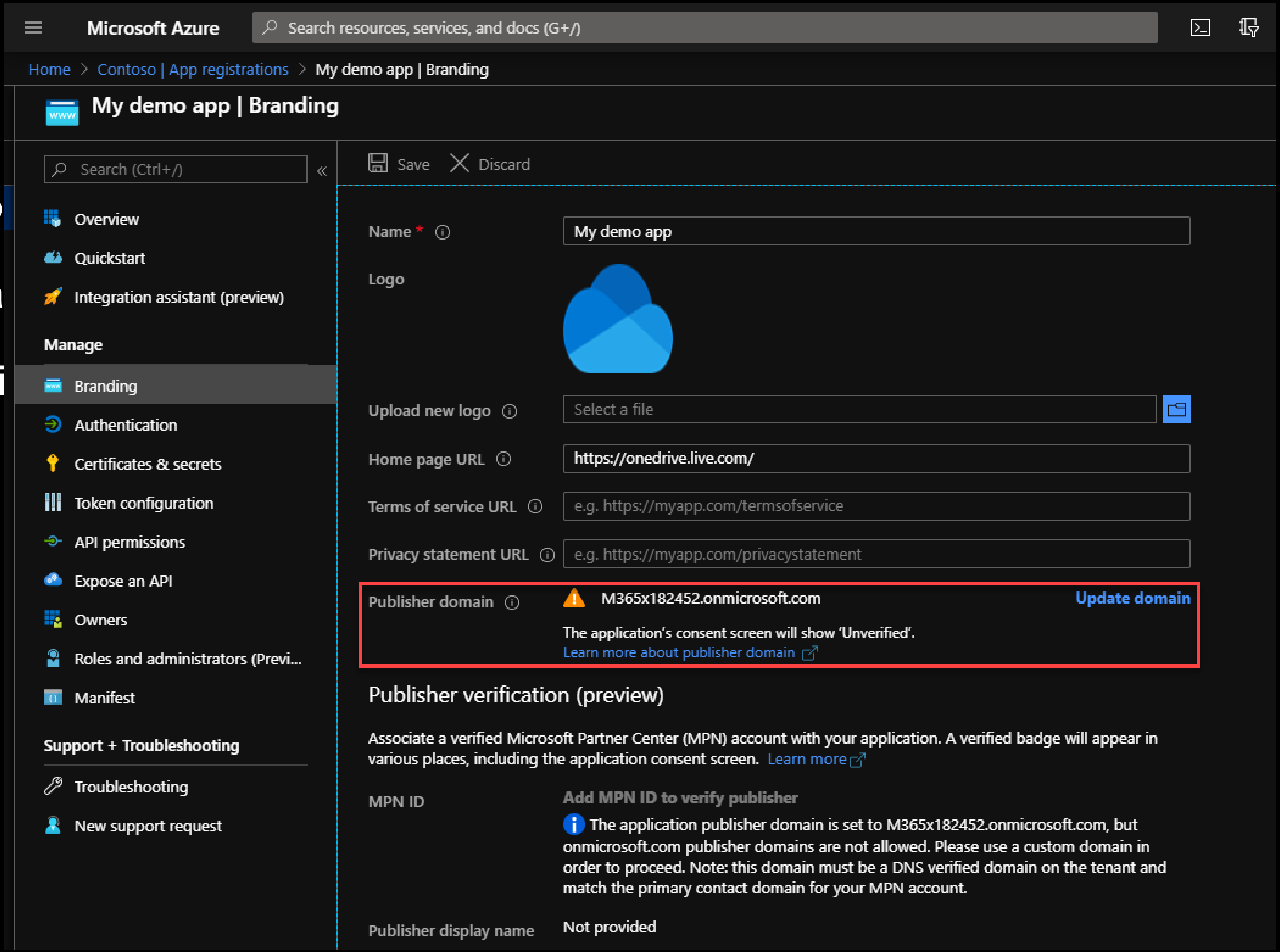
1 - 3 of 3 Policies

| Policy | Count | Severity | Category | Action |
|---|---|---|---|---|
| Malicious OAuth app consent<br>This policy uses Microsoft Threat Intelligence to scan OAuth apps connected t... | 0 open alerts | 🟥🟥🟥 | Threat detection | |
| Misleading publisher name for an OAuth app<br>This policy scans the OAuth apps connected to your environment and triggers... | 0 open alerts | 🟨⬜⬜ | Threat detection | |
| Misleading OAuth app name<br>This policy scans the OAuth apps connected to your environment and triggers... | 0 open alerts | 🟨⬜⬜ | Threat detection | |

# Application

Configure “Pub

- End-user ca
- MCAS polici



## My demo app | Branding

Name * My demo app

Logo

Upload new logo: Select a file

Home page URL: https://onedrive.live.com/

Terms of service URL: e.g. https://myapp.com/termsofservice

Privacy statement URL: e.g. https://myapp.com/privacystatement

Publisher domain: M365x182452.onmicrosoft.com

The application’s consent screen will show ‘Unverified’.
Learn more about publisher domain

### Publisher verification (preview)

Associate a verified Microsoft Partner Center (MPN) account with your application. A verified badge will appear in various places, including the application consent screen. Learn more

MPN ID: Add MPN ID to verify publisher

The application publisher domain is set to M365x182452.onmicrosoft.com, but onmicrosoft.com publisher domains are not allowed. Please use a custom domain in order to proceed. Note: this domain must be a DNS verified domain on the tenant and match the primary contact domain for your MPN account.

Publisher display name: Not provided

# Service Principal vs. Application

## Service Principal

“To access resources that are secured by an Azure AD tenant, the entity that requires access must be represented by a security principal. This is true for both users (user principal) and applications (service principal).

The security principal defines the access policy and permissions for the user/application in the Azure AD tenant. This enables core features such as authentication of the user/application during sign-in, and authorization during resource access.”

- Configuration:
  - Properties (Enabled, assignment etc.)
  - Owners
  - Users and groups
  - Etc.

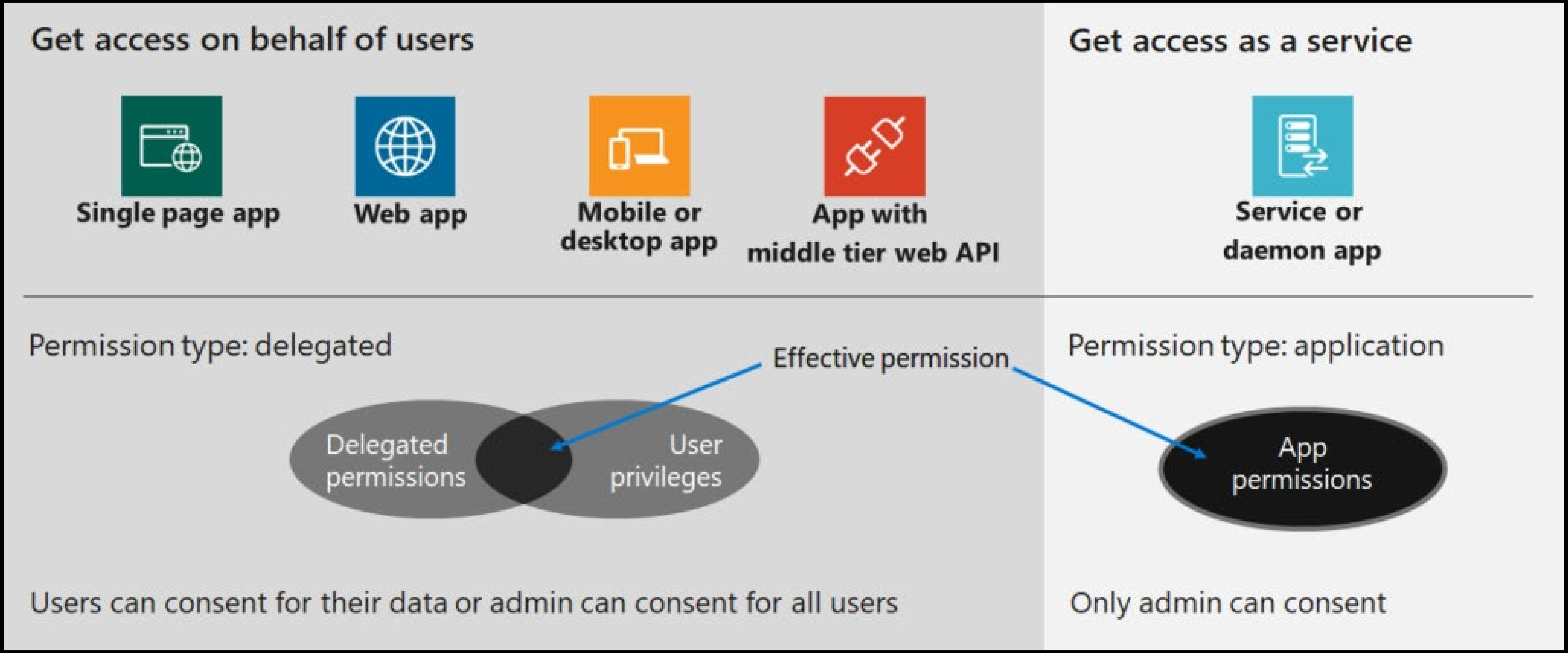
## Application

“An Azure AD application is defined by its one and only application object, which resides in the Azure AD tenant where the application was registered, known as the application's "home" tenant. The Microsoft Graph Application entity defines the schema for an application object's properties.”

- Configuration:
  - Branding
  - Authentication
  - API permissions
  - Etc.

# Delegated vs. Application permissions

**Credit: Microsoft**



# Delegated vs. Application permissions

## Delegated (on behalf of)

Delegated permissions, sometimes called “on behalf of” permissions, require a user context to also be supplied when making the request.  In effect an application is making Microsoft Graph requests on behalf of the user.  As such, the required permissions will be a combination of 1) what the user has permissions to do and 2) what the application has permissions to do.

The logical intersection of these two results in the effective permissions used when making requests.  If the application has been granted permissions (ex. read all user info from Azure AD) that the user has not been granted, then the application will not be able to complete that specific request.

If you are decoding an access token, delegated permissions will show up as “scopes” within the decoded claims.  Checking that the access token has the appropriate / expected “scopes” is a good first step to ensure that permissions are assigned and consented.

## Application (app-only or “without a user”)

Application permissions, sometimes called app-only or “without a user”, run without a user context.  Common examples of this would be a background service or a daemon application.  Only the permissions granted to the application will be evaluated when Microsoft Graph request is made.

Typically an Azure AD domain administrator needs to grant consent for the application permissions requested.  However, there is a new Azure AD role called Application Administrator that is able to consent to delegated permissions for Azure AD apps, and applications permissions excluding Microsoft Graph and Azure AD Graph.  For the purposes of this blog series that may not be suitable given the Microsoft Graph exclusion but it is worth noting for other scenarios.  Read more about available roles for Administrator role permissions in Azure Active Directory.

If you are decoding an access token, application permissions will show up as “roles” within the decoded claims.  Checking that the access token has the appropriate / expected “roles” is a good first step to ensure that permissions are assigned and consented.

# Exchange protocols

Exchange Web Services (EWS)

- Long existing protocol
- Managed API (DLL) for installation
- SOAP requests
- Full functionality (in terms of access and configuration of mailbox)

REST

- Relatively young protocol
- OData 4.0 and JSON for data abstraction
- Optimized for accessing mail, calendar and contacts
- Supports ONLY OAuth for authentication and authorization
- Limited functionality (in terms of access and configuration of mailbox)

# Endpoints for Exchange Online

There are different endpoints, which can be used for accessing Exchange objects:

Note: In OAuth terms these are also know as Audience/Resource.

- Microsoft Graph (https://graph.microsoft.com)
- Exchange Online (https://outlook.office365.com)

These endpoints have different capabilities.

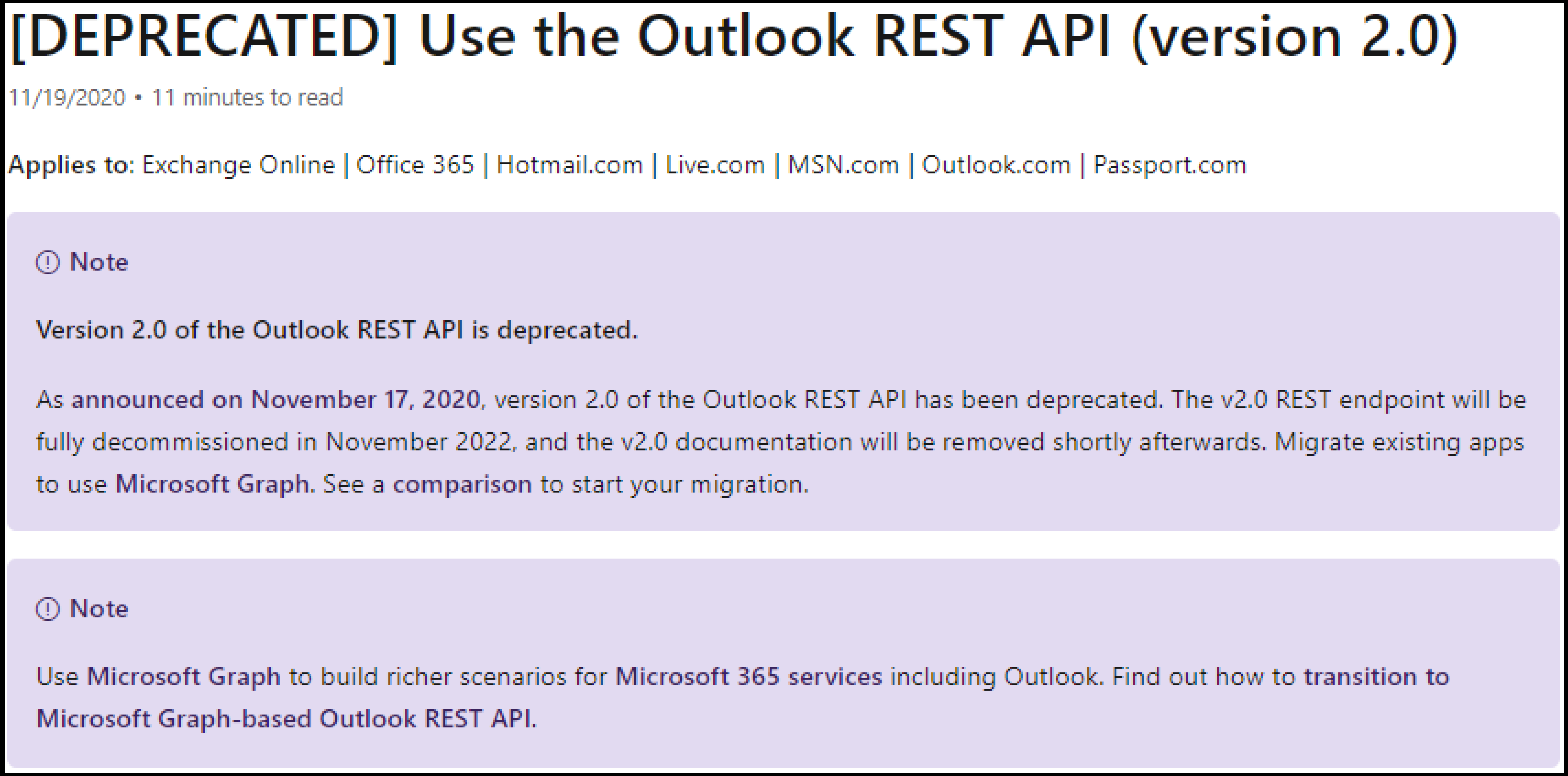
- Microsoft Graph doesn't have Application permissions for:
  - EWS
  - IMAP
  - EAS
  - Etc.

There are also more feature differences outlined here:

https://docs.microsoft.com/outlook/rest/compare-graph#feature-differences

Note: This needs to be taken into consideration, while creating an application architecture!

# Endpoints for Exchange Online



## [DEPRECATED] Use the Outlook REST API (version 2.0)

11/19/2020 • 11 minutes to read

**Applies to:** Exchange Online | Office 365 | Hotmail.com | Live.com | MSN.com | Outlook.com | Passport.com

ⓘ Note

**Version 2.0 of the Outlook REST API is deprecated.**

As announced on November 17, 2020, version 2.0 of the Outlook REST API has been deprecated. The v2.0 REST endpoint will be fully decommissioned in November 2022, and the v2.0 documentation will be removed shortly afterwards. Migrate existing apps to use Microsoft Graph. See a comparison to start your migration.

ⓘ Note

Use Microsoft Graph to build richer scenarios for Microsoft 365 services including Outlook. Find out how to transition to Microsoft Graph-based Outlook REST API.

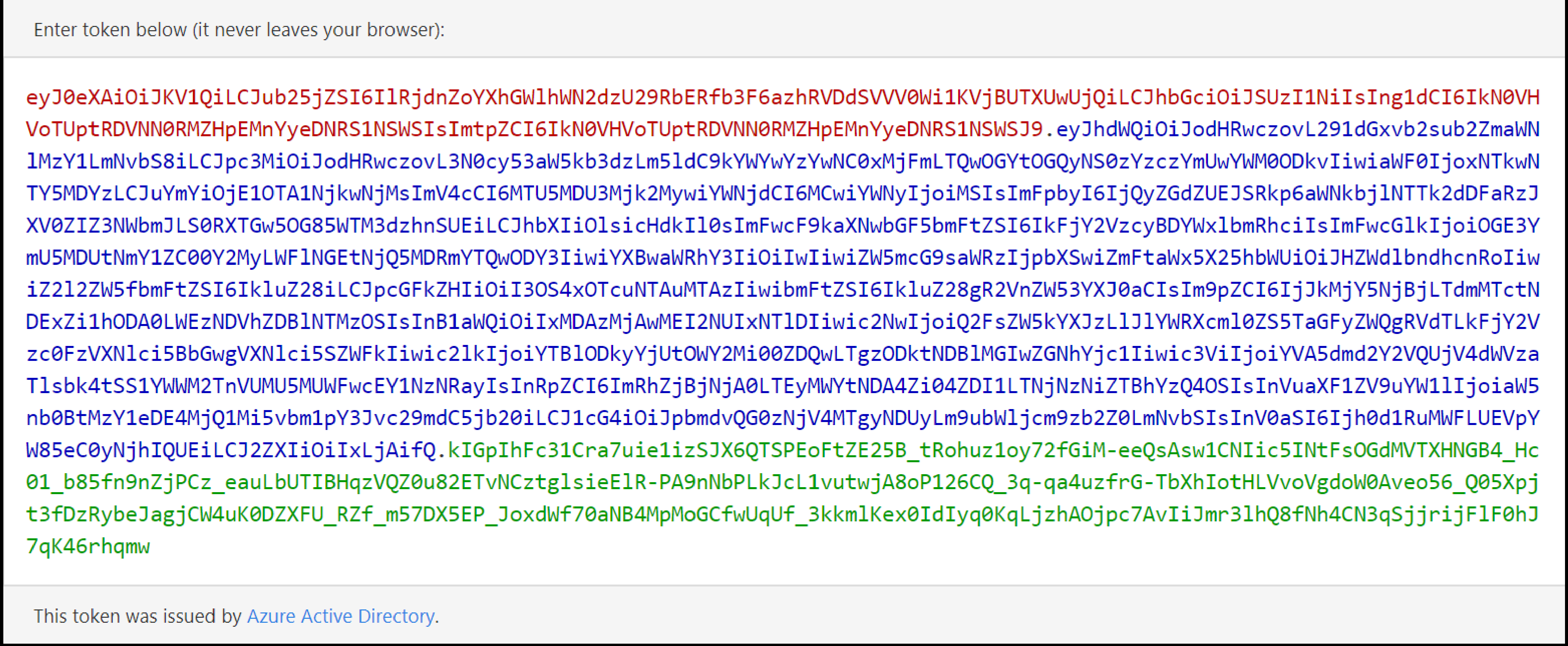
# Decoding Access Token

- ADFS Help JWT Decoder
- https://jwt.ms/
- https://jwt.io/

Full documentation about claims:

Microsoft identity platform access tokens

# Example JWT.ms

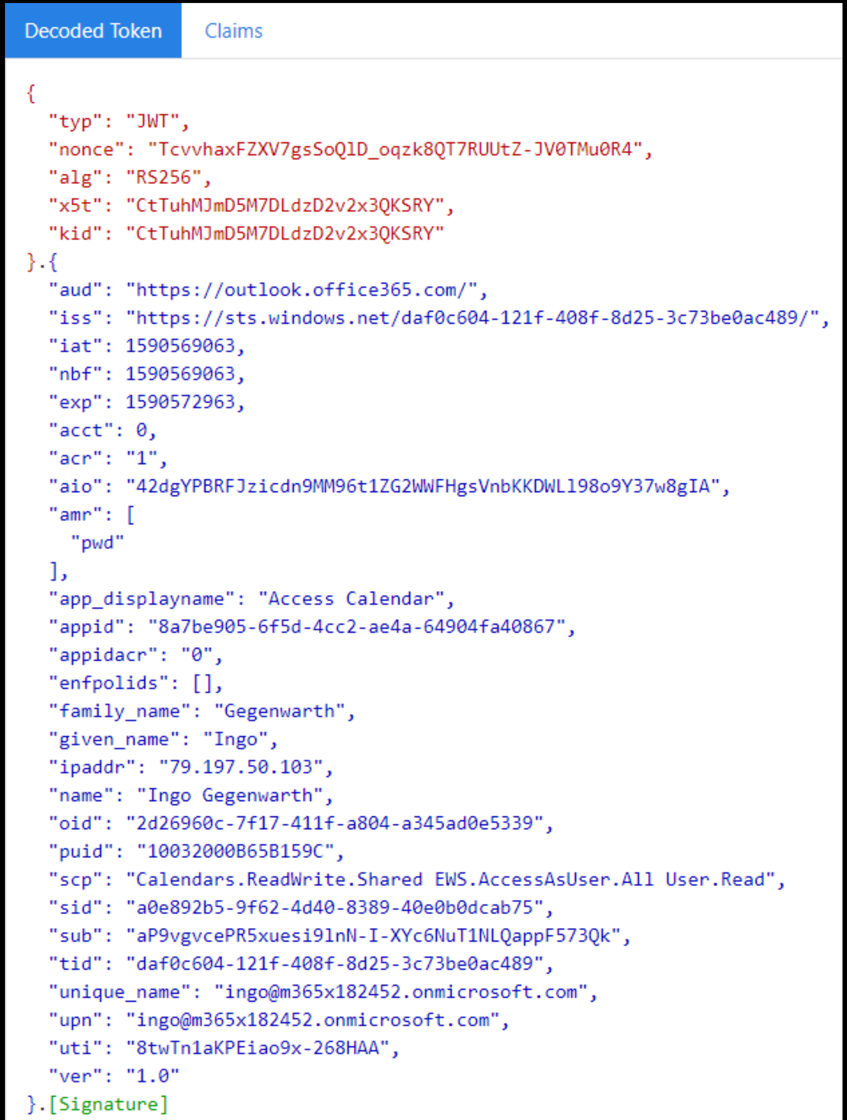


Enter token below (it never leaves your browser):

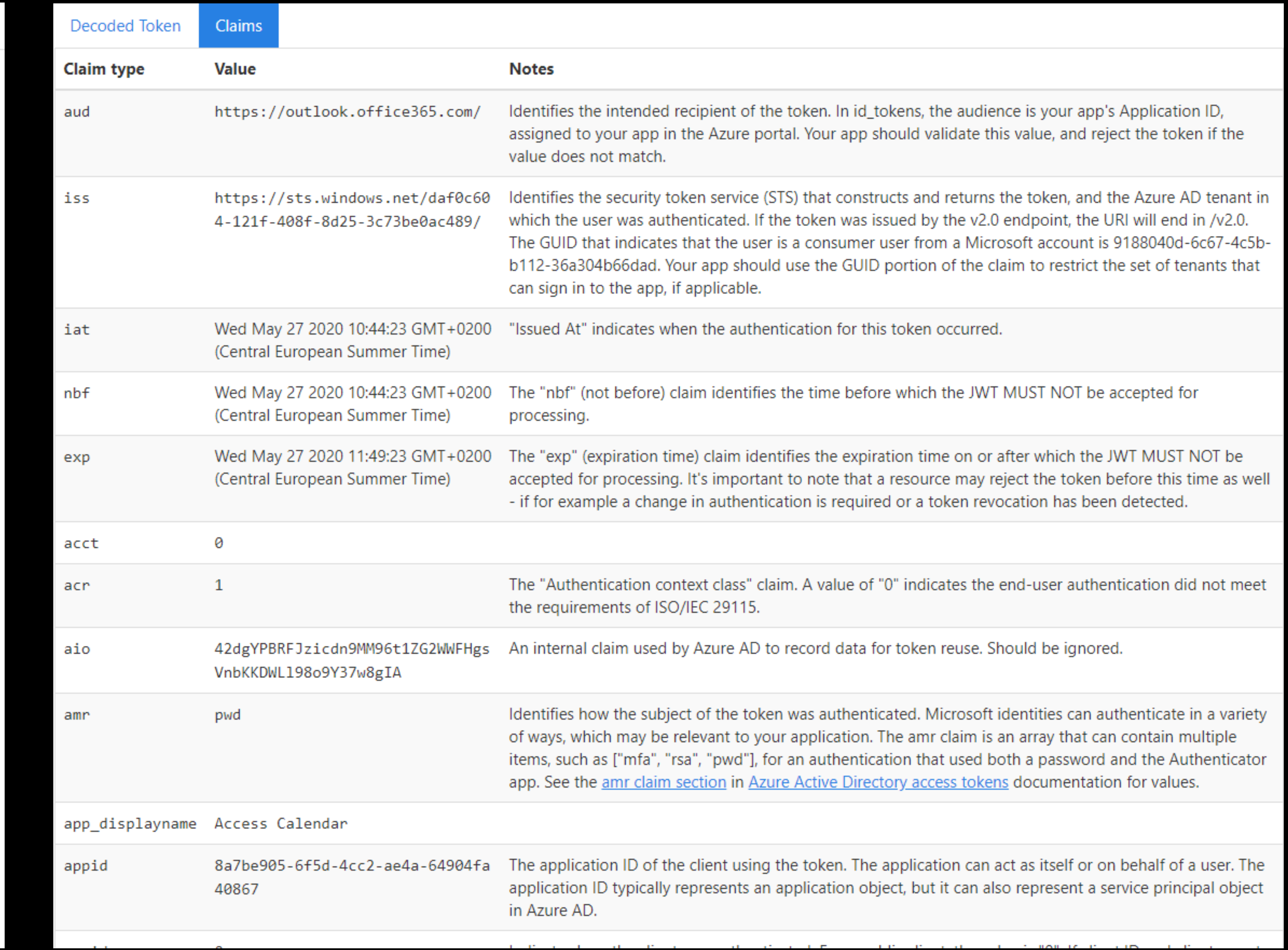
```
eyJ0eXAiOiJKV1QiLCJub25jZSI6IlRjdnZoYXhGWlhWN2dzU29RbERfb3F6azhRVDdSVVV0Wi1KVjBUTXUwUjQiLCJhbGciOiJSUzI1NiIsIng1dCI6IkN0VH
VoTUptRDVNN0RMZHpEMnYyeDNRS1NSWSIsImtpZCI6IkN0VHVoTUptRDVNN0RMZHpEMnYyeDNRS1NSWSJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWN
lMzY1LmNvbS8iLCJpc3MiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC9kYWYwYzYwNC0xMjFmLTQwOGYtOGQyNS0zYzczYmUwYWM0ODkvIiwiaWF0IjoxNTkwN
TY5MDYzLCJuYmYiOjE1OTA1NjkwNjMsImV4cCI6MTU5MDU3Mjk2MywiYWNjdCI6MCwiYWNyIjoiMSIsImFpbyI6IjQyZGdZUEJSRkp6aWNkbjlNTTk2dDFaRzJ
XV0ZIZ3NWbmJLS0RXTGw5OG85WTM3dzhnSUEiLCJhbXIiOlsicHdkIl0sImFwcF9kaXNwbGF5bmFtZSI6IkFjY2VzcyBDYWxlbmRhciIsImFwcGlkIjoiOGE3Y
mU5MDUtNmY1ZC00Y2MyLWFlNGEtNjQ5MDRmYTQwODY3IiwiYXBwaWRhY3IiOiIwIiwiZW5mcG9saWRzIjpbXSwiZmFtaWx5X25hbWUiOiJHZWdlbndhcnRoIiw
iZ2l2ZW5fbmFtZSI6IkluZ28iLCJpcGFkZHIiOiI3OS4xOTcuNTAuMTAzIiwibmFtZSI6IkluZ28gR2VnZW53YXJ0aCIsIm9pZCI6IjJkMjY5NjBjLTdmMTctN
DExZi1hODA0LWEzNDVhZDBlNTMzOSIsInB1aWQiOiIxMDAzMjAwMEI2NUIxNTlDIiwic2NwIjoiQ2FsZW5kYXJzLlJlYWRXcml0ZS5TaGFyZWQgRVdTLkFjY2V
zc0FzVXNlci5BbGwgVXNlci5SZWFkIiwic2lkIjoiYTBlODkyYjUtOWY2Mi00ZDQwLTgzODktNDBlMGIwZGNhYjc1Iiwic3ViIjoiYVA5dmd2Y2VQUjV4dWVza
Tlsbk4tSS1YWWM2TnVUMU5MUWFwcEY1NzNRayIsInRpZCI6ImRhZjBjNjA0LTEyMWYtNDA4Zi04ZDI1LTNjNzNiZTBhYzQ4OSIsInVuaXF1ZV9uYW1lIjoiaW5
nb0BtMzY1eDE4MjQ1Mi5vbm1pY3Jvc29mdC5jb20iLCJ1cG4iOiJpbmdvQG0zNjV4MTgyNDUyLm9ubWljcm9zb2Z0LmNvbSIsInV0aSI6Ijh0d1RuMWFLUEVpY
W85eC0yNjhIQUEiLCJ2ZXIiOiIxLjAifQ.kIGpIhFc31Cra7uie1izSJX6QTSPEoFtZE25B_tRohuz1oy72fGiM-eeQsAsw1CNIic5INtFsOGdMVTXHNGB4_Hc
01_b85fn9nZjPCz_eauLbUTIBHqzVQZ0u82ETvNCztglsieElR-PA9nNbPLkJcL1vutwjA8oP126CQ_3q-qa4uzfrG-TbXhIotHLVvoVgdoW0Aveo56_Q05Xpj
t3fDzRybeJagjCW4uK0DZXFU_RZf_m57DX5EP_JoxdWf70aNB4MpMoGCfwUqUf_3kkmlKex0IdIyq0KqLjzhAOjpc7AvIiJmr3lhQ8fNh4CN3qSjjrijFlF0hJ
7qK46rhqmw
```

This token was issued by Azure Active Directory.

# Example JWT.ms



```
{
  "typ": "JWT",
  "nonce": "TcvvhaxFZXV7gsSoQ1D_oqzk8QT7RUUtZ-JV0TMu0R4",
  "alg": "RS256",
  "x5t": "CtTuhMJmD5M7DLdzD2v2x3QKSRY",
  "kid": "CtTuhMJmD5M7DLdzD2v2x3QKSRY"
}.{
  "aud": "https://outlook.office365.com/",
  "iss": "https://sts.windows.net/daf0c604-121f-408f-8d25-3c73be0ac489/",
  "iat": 1590569063,
  "nbf": 1590569063,
  "exp": 1590572963,
  "acct": 0,
  "acr": "1",
  "aio": "42dgYPBRFJzicdn9MM96t1ZG2WWFHgsVnbKKDWLl98o9Y37w8gIA",
  "amr": [
    "pwd"
  ],
  "app_displayname": "Access Calendar",
  "appid": "8a7be905-6f5d-4cc2-ae4a-64904fa40867",
  "appidacr": "0",
  "enfpolids": [],
  "family_name": "Gegenwarth",
  "given_name": "Ingo",
  "ipaddr": "79.197.50.103",
  "name": "Ingo Gegenwarth",
  "oid": "2d26960c-7f17-411f-a804-a345ad0e5339",
  "puid": "10032000B65B159C",
  "scp": "Calendars.ReadWrite.Shared EWS.AccessAsUser.All User.Read",
  "sid": "a0e892b5-9f62-4d40-8389-40e0b0dcab75",
  "sub": "aP9vgvcePR5xuesi9lnN-I-XYc6NuT1NLQappF573Qk",
  "tid": "daf0c604-121f-408f-8d25-3c73be0ac489",
  "unique_name": "ingo@m365x182452.onmicrosoft.com",
  "upn": "ingo@m365x182452.onmicrosoft.com",
  "uti": "8twTn1aKPEiao9x-268HAA",
  "ver": "1.0"
}.[Signature]
```



| Claim type | Value | Notes |
|---|---|---|
| aud | https://outlook.office365.com/ | Identifies the intended recipient of the token. In id_tokens, the audience is your app's Application ID, assigned to your app in the Azure portal. Your app should validate this value, and reject the token if the value does not match. |
| iss | https://sts.windows.net/daf0c604-121f-408f-8d25-3c73be0ac489/ | Identifies the security token service (STS) that constructs and returns the token, and the Azure AD tenant in which the user was authenticated. If the token was issued by the v2.0 endpoint, the URI will end in /v2.0. The GUID that indicates that the user is a consumer user from a Microsoft account is 9188040d-6c67-4c5b-b112-36a304b66dad. Your app should use the GUID portion of the claim to restrict the set of tenants that can sign in to the app, if applicable. |
| iat | Wed May 27 2020 10:44:23 GMT+0200 (Central European Summer Time) | "Issued At" indicates when the authentication for this token occurred. |
| nbf | Wed May 27 2020 10:44:23 GMT+0200 (Central European Summer Time) | The "nbf" (not before) claim identifies the time before which the JWT MUST NOT be accepted for processing. |
| exp | Wed May 27 2020 11:49:23 GMT+0200 (Central European Summer Time) | The "exp" (expiration time) claim identifies the expiration time on or after which the JWT MUST NOT be accepted for processing. It's important to note that a resource may reject the token before this time as well - if for example a change in authentication is required or a token revocation has been detected. |
| acct | 0 | |
| acr | 1 | The "Authentication context class" claim. A value of "0" indicates the end-user authentication did not meet the requirements of ISO/IEC 29115. |
| aio | 42dgYPBRFJzicdn9MM96t1ZG2WWFHgsVnbKKDWLl98o9Y37w8gIA | An internal claim used by Azure AD to record data for token reuse. Should be ignored. |
| amr | pwd | Identifies how the subject of the token was authenticated. Microsoft identities can authenticate in a variety of ways, which may be relevant to your application. The amr claim is an array that can contain multiple items, such as ["mfa", "rsa", "pwd"], for an authentication that used both a password and the Authenticator app. See the amr claim section in Azure Active Directory access tokens documentation for values. |
| app_displayname | Access Calendar | |
| appid | 8a7be905-6f5d-4cc2-ae4a-64904fa40867 | The application ID of the client using the token. The application can act as itself or on behalf of a user. The application ID typically represents an application object, but it can also represent a service principal object in Azure AD. |

“I acquired an access token.
Now I can access mailboxes
or send-as other users?”

# Working with Exchange Online objects

Delegated permissions:

- Permissions in EXO still needs to be granted (access token is not sufficient):
  - FullAccess
  - Send-As
  - Folder-level permission
  - Etc.

Application permissions:

- OAuth Application permissions ≠ ApplicationImpersonation permission (EWS)
- specific headers are still needed to be added:
  - **X-AnchorMailbox** (should meanwhile added in any cases)
  - **ExchangeImpersonation** SOAP

# Working with Exchange Online objects

Restrict applications:

- Conditional Access rules (AAD)
- Microsoft Cloud App Security (MCAS)

  Note: Only in combination with CA!
- ApplicationAccessPolicy (EXO)

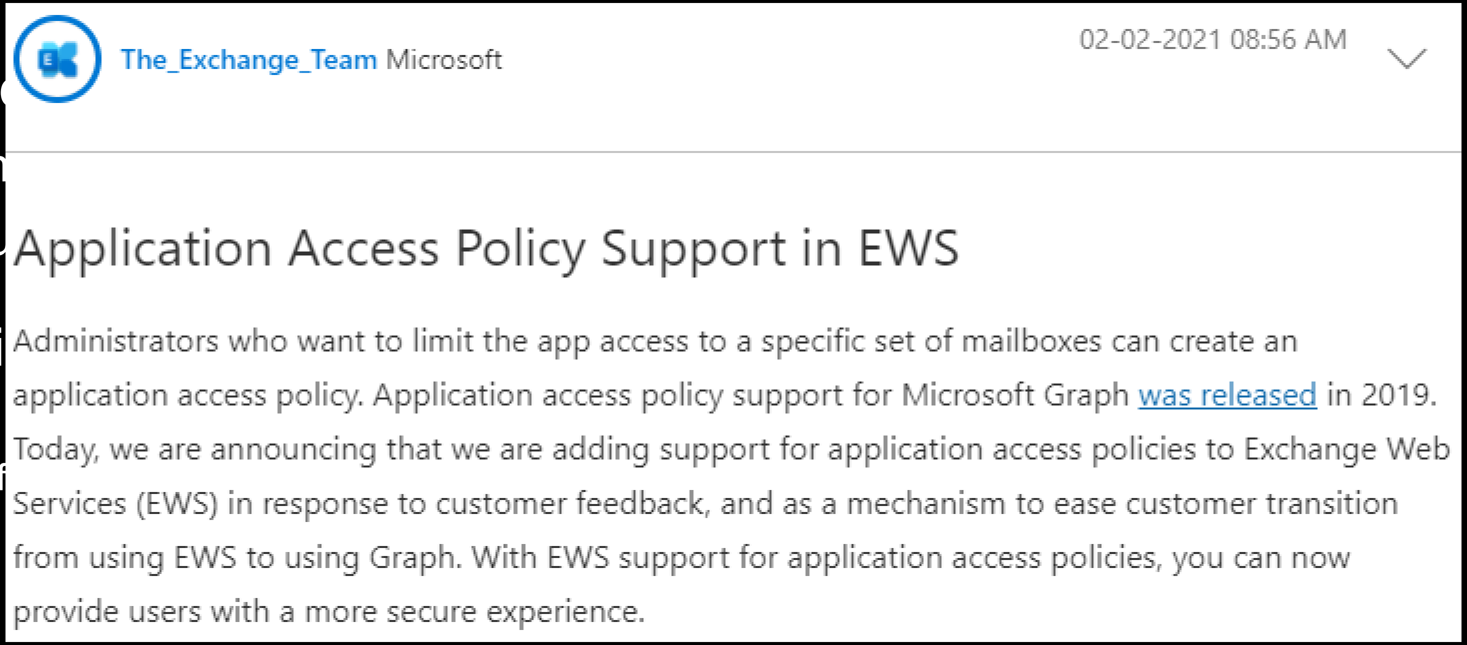
  Note: ApplicationAccessPolicy also work with Application permissions!

# Example:
# “We have an HR app, which should be used only for a subset of users.”

# Example

Possible solutions:

- Configure Servi
  - require assignm
  - assign SPN to u
- Create Applicati
  - Restrict access
    Note: Works ONLY f



The_Exchange_Team Microsoft

02-02-2021 08:56 AM

## Application Access Policy Support in EWS

Administrators who want to limit the app access to a specific set of mailboxes can create an application access policy. Application access policy support for Microsoft Graph was released in 2019. Today, we are announcing that we are adding support for application access policies to Exchange Web Services (EWS) in response to customer feedback, and as a mechanism to ease customer transition from using EWS to using Graph. With EWS support for application access policies, you can now provide users with a more secure experience.

# Wrap up

- Tenant-wide configuration
  - Illicit Consent Grants
  - Configure how end-users consent to applications
  - Conditional Access/MCAS
- Service Principal/Application configuration
- Exchange Online:
  - EWS/REST protocol
  - Client Access Rule
- Access token and recipient permissions:
  - How to request an access token
  - I now have an access token. Now I’m good to go?

# Tooling

- Postman:
  - Made for API Development
  - Query collection available on GitHub (Azure AD documentation can be found here!)
- Microsoft Graph PowerShell Module
  - Easy to install from repository PowerShell Gallery
- MSAL.PS PowerShell module
- ADAL.PS PowerShell module
- Get-AccessToken

# Appendix

Managing consent to applications and evaluating consent requests

Configure how end-users consent to applications

Detect and Remediate Illicit Consent Grants

Client Access Rules in Exchange Online

Exchange Online protocols:

- Exchange Web Services
- REST
- Scoping applications in Exchange Online
- Supported permissions for scoping

Microsoft Graph Explorer

Microsoft Graph PowerShell module

OAuth basics:

- Authentication vs. authorization
- Application types for Microsoft identity platform
- Authentication flows and application scenarios

MCAS:

- Managing risky 3rd party app permissions with Microsoft's CASB
- Manage OAuth apps

Compare Graph and Outlook