
NIC
REBEL
EDITION

Jan Ketil Skanke

Getting Started with MS Graph API for the IT Admin

NIC REBEL EDITION

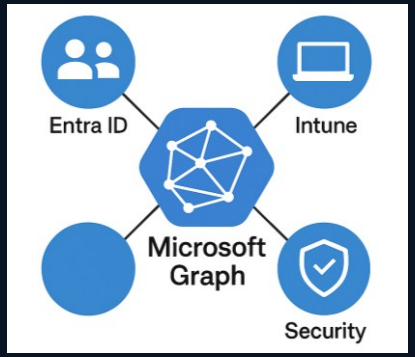
Jan Ketil Skanke

- Principal Cloud Architect - CloudWay
- Microsoft MVP in Security (Identity and AccessMgmt + Intune)
- SocialMedia @JankeSkanke

- Star Wars, Lego and Formula 1 Geek

NIC REBEL EDITION

What is Microsoft Graph?



- **Microsoft Graph** is a unified API endpoint provided by Microsoft that allows us to access data, and intelligence across Microsoft 365 services. We can also do actions via the API
- Essentially, it connects multiple Microsoft cloud services through a single REST API, enabling integration, automation, and insights.

NIC REBEL EDITION

Requesting Data from MS Graph API

- Query methods to use:
  - GET, POST, PUT, PATCH, DELETE
- Construct a URI pointing to a Graph API endpoint including resources
  - Query parameters
    - $filter, $expand, $select, $top, $skip and more
    - Limitations to query parameters:
      - https://learn.microsoft.com/en-us/graph/known-issues?view=graph-rest-1.0#query-parameters
- Headers and Body
  - Header primarily contains access token
  - For certain resources, additional headers must be embedded:
    - consistencylevel = eventual
    - These are well documented when needed
  - Body is used for when adding or changing resources (POST, PATCH)

NIC REBEL EDITION

Microsoft Graph – Query Format

GET	POST	PUT	PATCH	DELETE
Provides the ability to pull data from Microsoft Graph	Provides the ability to POST / ADD data into Microsoft Graph	Provides the ability to PUT / ASSIGN data into Microsoft Graph	Provides the ability to PATCH / UPDATE resources	Provides the ability to DELETE individual resources from Microsoft Graph
Data returned in JSON format	Data sent to the service in JSON format	Data sent to the service in JSON format	Data sent to the service in JSON format	

NIC REBEL EDITION

Tools to Interact with MS Graph

- Graph Explorer
- Graph X-Ray
- PowerShell or other languages

NIC REBEL EDITION

Define a URI

```
https://graph.microsoft.com /{endpoint} /{resource} ?{query-parameters}

https://graph.microsoft.com /v1.0/deviceManagement/managedDevices ?$top=10


https://graph.microsoft.com /{endpoint} /{resource} /{id}

https://graph.microsoft.com /beta /deviceManagement/managedDevices /bc841xxxxxxxx
```

NIC REBEL EDITION

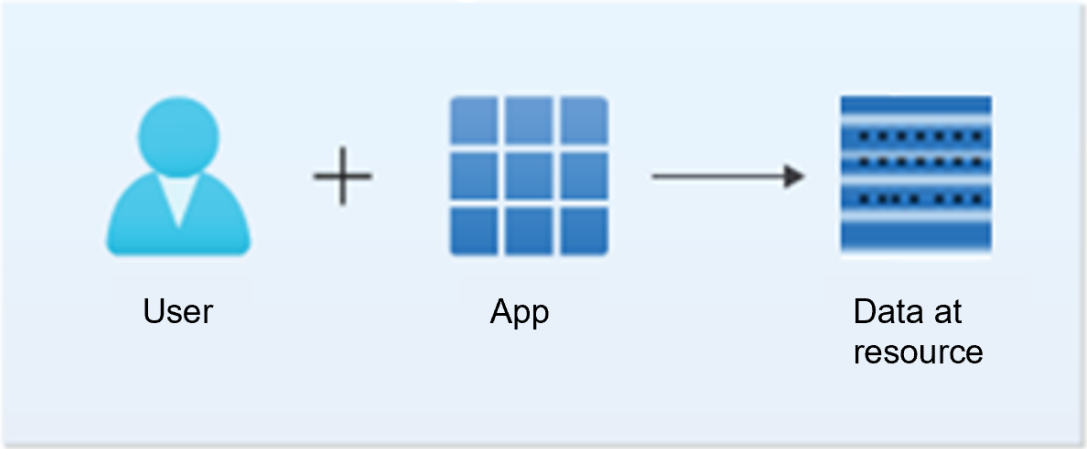
Introductions to Microsoft Graph API

- Graph is “everywhere”
- Find the API Calls to use

NIC REBEL EDITION

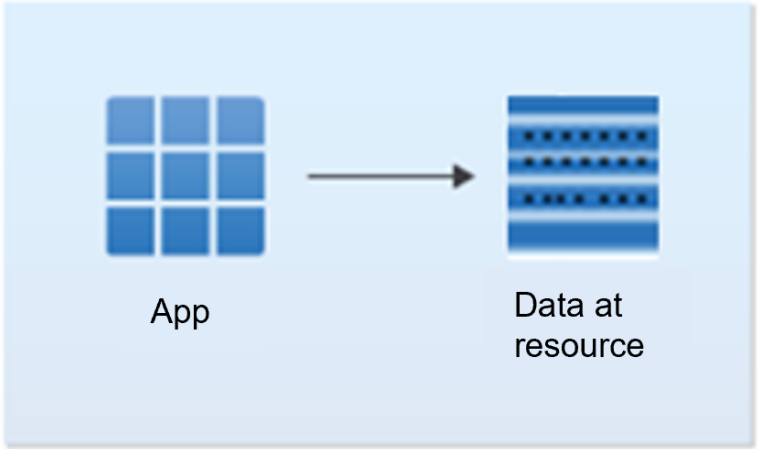
Scopes (a.k.a permissions)

Delegated access



“Access on behalf of a user”

App-only access



“Access without a user”

NIC REBEL EDITION

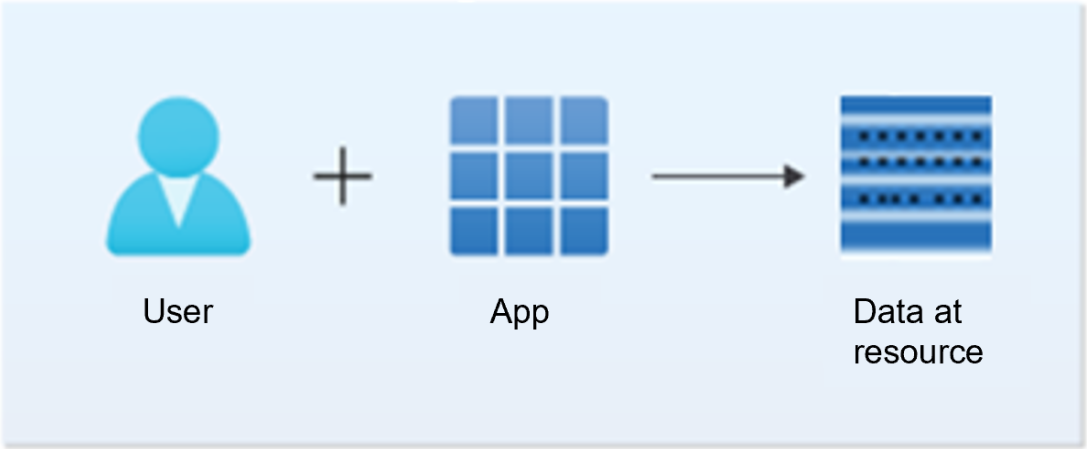
Scopes (a.k.a permissions)

- Scopes definition:
  - Permissions and operations an application has access to for a given resource
- Scopes can be granted to resources in the follow ways:
  - Delegated access
    - Access performed on behalf of a user
    - Application specifically asks the user to grant the defined scopes
    - Use delegated access when you want the user to perform operational tasks
- App-only access
  - Application accesses resources directly, e.g. Microsoft Graph
  - Admin should grant consent for this type of access (not all scopes requires consent)
  - Use application access when there's a need for automating operational tasks

NIC REBEL EDITION

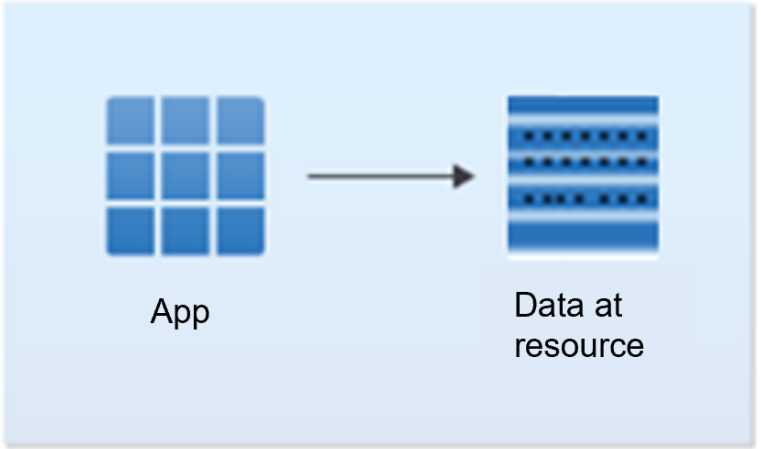
Scopes (a.k.a permissions)

Delegated access



“Access on behalf of a user”

App-only access



“Access without a user”

NIC REBEL EDITION

Graph API Permissions

- Recommendations
  - Least privilege rule applies
  - Generic Graph app for interactive use
  - Unique application registration per automation solution (Least privilege..)

NIC REBEL EDITION

Authentication Methods

NIC REBEL EDITION

Authentication Methods

- Connecting to Microsoft Graph
  - Interactive, Device Code, Certificates
  - Non-Interactive
  - Using Entra ID Application Registration for Access
- Authentication Flows
- Tokens

NIC REBEL EDITION

Authentication flows

Authentication flow	Type	Access Type	Use-cases
Authorization Code	Interactive	Delegated	On-demand requiring interactive sign-in
Device Code	Interactive	Delegated	On-demand requiring interactive sign-in on separate device
Client Credentials (client secret)	Non-interactive	Application	Unattended automation such as Azure Automation or Function Apps with secret in Key Vault
Client Credentials (certificate)	Non-interactive	Application	Unattended automation, similar to client secret flow usage

NIC REBEL EDITION

Access token

Access tokens are required for using Graph API. Also known as the bearer token, which means the token is already verified when issued, letting any bearer of the token use it.

Short validity period

Refresh token

When acquiring an access token, a refresh token is also received. Has a longer validity period and is used to retrieve a new access token and refresh token pair for when the access token expires.

Longer validity period

Id token

Third token that comes with the OpenID Connect extension. Contains details about the user or identity that the token belongs to, enabling SSO or e.g. proving the identity of someone to a third party, for example Azure DevOps.

Extension token

NIC REBEL EDITION

Permissions and Consent

- App Registration
- Native App

NIC REBEL EDITION

PowerShell and Graph API

NIC REBEL EDITION

NIC REBEL EDITION