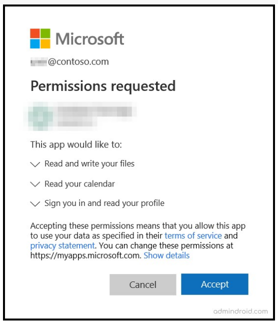
App Permissions & Consents in Microsoft 365 (M365)

Version 2

Published 7/15/2024 by Giuseppe Aloisi Last updated 7/15/2024 7:21 PM by Giuseppe Aloisi

Third-party services offer Single Sign-On (SSO) which allows the use of Seneca credentials to authenticate their applications. However, this can pose a security and privacy risk if the applications are not vetted carefully.

The M365 Preapproved Apps Policy at Seneca Polytechnic is designed to ensure the security and integrity of our digital environment by allowing only Seneca-approved applications that are considered low-risk to accept Seneca credentials for authentication



Microsoft

[redacted]@contoso.com

Permissions requested

[redacted]

This app would like to:

- Read and write your files
- Read your calendar
- Sign you in and read your profile

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

***image above shows a prompt required for o365 SSO applications' required permissions with an accept or cancel button.*

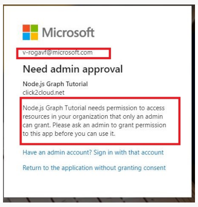
Policy Overview:

1. Preapproved Apps:

- Only applications approved by Seneca IT are allowed within the M365 environment. These applications are considered low-risk and have undergone thorough security assessments.
- Users are encouraged to explore preapproved apps available to enhance their productivity and user experience.
- These applications will not require users to accept further privacy agreements or grant permissions.

2. Apps requiring approval:

- Any application prompting for approval must go through a review process.
- Users attempting to install these apps and authenticate using Seneca credentials will be notified to contact Seneca Polytechnic IT for a security and compliance review



Microsoft

v-rogavf@microsoft.com

Need admin approval

Node.js Graph Tutorial
click2cloud.net

Node.js Graph Tutorial needs permission to access resources in your organization that only an admin can grant. Please ask an admin to grant permission to this app before you can use it.

Have an admin account? Sign in with that account
Return to the application without granting consent

** The image above shows a prompt for the user to reach out to IT administration for application approval.

3. App review and approval process:

- Users seeking to use an app not preapproved by Seneca must contact IT support for assistance.
- Contact itsapp.approval@senecapolytechnic.ca with your application request and valid business case for the application
- The IT approval team will conduct a comprehensive review of the requested application, considering factors such as security, data privacy, and compatibility with Seneca systems.
- Approvals may take up to 5 business days (excluding holidays) to review

4. Approval Process:

- Upon receiving a request, IT support will evaluate the proposed application.
- The review process will include an assessment of the application's security features, compliance with Seneca's policies, and potential impact on the IT infrastructure.
- Users will be informed of the approval or denial of their application request.
- Please note that a user can always authenticate against any third-party applications using credentials not associated with Seneca

5. Educational Outreach:

- Seneca Polytechnic IT will provide educational resources to help users understand the importance of using preapproved apps and the potential risks associated with unauthorized applications.
- Training sessions and workshops may be organized to keep the Seneca community informed about the latest cyber security threats and best practices.