Olyteck Cyber
Cybersecurity for Microsoft 365

MICROSOFT GRAPH · SCOPE-BY-SCOPE

Graph API permissions

Every Microsoft Graph permission Olyteck Cyber requests, with the business justification. Tenant administrators see this list on the consent screen prior to grant.

Posture	Read-only by default. The product reads configuration and permission metadata; it does not retrieve file content or e-mail bodies.
Consent model	Initial admin consent by a Global Administrator (or equivalent). Day-to-day operation does not require Global Administrator.
Revocation	A tenant administrator can revoke the application's consent at any time in the Microsoft 365 admin centre.
Version	1.0 - 29 May 2026

Sign-in application (delegated)

Used purely to identify the user signing in to Olyteck Cyber. No customer content is accessed under this consent.

Scope	Type	Why
openid	Delegated	OpenID Connect sign-in
profile	Delegated	Basic profile (name, locale)
email	Delegated	User's primary e-mail for support contact
offline_access	Delegated	Refresh tokens to keep the session alive without re-prompting
User.Read	Delegated	Read the signed-in user's profile

Scanner application (admin-consented)

Read-oriented Graph permissions sufficient to evaluate the security posture surfaces described in the main Security and Architecture Documentation.

Scope	Type	Why we request it
Directory.Read.All	Application	Read tenant identity posture: MFA registration, guest accounts, admin role assignments, dormant licensed users.
AuditLog.Read.All	Application	Read sign-in activity and audit logs to detect dormant users and risky sign-ins (Tenant posture module).
Policy.Read.All	Application	Read Conditional Access policies and the CA scorecard inputs (legacy auth, MFA for admins, high-risk block, compliant device).
Group.Read.All	Application	Read group and Microsoft 365 group memberships (used by SharePoint, Teams, and identity modules).
Team.ReadBasic.All	Application	Enumerate Teams to evaluate channel permissions and external membership via the backing SharePoint sites.
Sites.Read.All	Application	Read SharePoint sites, drives, sharing links, and ownership (SharePoint and Teams modules).
Files.Read.All	Application	Read OneDrive for Business quotas, sharing links, and drive items (OneDrive module). The product reads metadata only - it does not download file content.
MailboxSettings.Read	Application	Read mailbox inbox rules to detect the highest-signal indicator of business e-mail compromise (Email security module).
Reports.Read.All	Application	Read M365 usage reports (Copilot readiness, dormant licence detection, storage thresholds).
IdentityRiskyUser.Read.All	Application	Read identity-protection risky-user signals (Identity posture module). Skipped if the tenant does not license Identity Protection.
Application.Read.All	Application	Enumerate enterprise applications and service principals to flag unverified publishers and risky OAuth scopes (OAuth apps module).

Permissions deliberately not requested

- No Mail.Read or Mail.ReadWrite - we read inbox rules, never mailbox contents.
- No Files.ReadWrite.All - the product does not modify customer files.
- No Directory.ReadWrite.All - the product does not modify directory objects.
- No Sites.FullControl.All - the product does not require full SharePoint control.

Customer controls

If the customer's policy prohibits any specific scope on the list above, contact support@olyteck.com so that we can identify which modules would be affected and whether a restricted-scope configuration is appropriate.

Issued as-is

This permissions statement is issued by Olyteck and may be relied upon as-is during prospect evaluation and procurement. A counter-signed copy is provided on customer request as part of the contracting paperwork.