

ENDPOINT ASSURANCE GROUP

Read-Only Assessment Access and Authorization

Least-privilege delegated access, tenant identity, evidence handling, and client approval.

PREPARED FOR

[Client Name]

PREPARED BY

John Jankowski

ORGANIZATION

[Client Organization]

EMAIL

john@endpointassurancegroup.com

DATE

[Month Day, Year]

VERSION

1.0

Client control: The client retains control of the account, consent, session, and revocation. No production configuration changes are authorized by this form.

Assessment identification

Field	Client response
Client organization	[Client Organization]
Engagement	[Intune Assurance / Acquisition Discovery / Both separately]
Expected tenant ID	[Complete 36-character GUID]
Approved operator account	[UPN]
Authorized assessment window	[Start / end date and time zone]
Client approver	[Name / title / email]
Evidence retention	[Period and disposition]

Requested delegated permissions

Permission	Purpose	Used when
User.Read	Verify the signed-in delegated identity	All engagements
DeviceManagementConfiguration.Read.All	Read Intune configuration, compliance, Settings Catalog, endpoint security, updates and assignments	Core, operations, conflicts and acquisition
DeviceManagementManagedDevices.Read.All	Read managed-device inventory and health state	Core, operations, duplicate devices and acquisition
DeviceManagementApps.Read.All	Read application inventory, assignments, protection and audit evidence	Core, applications, governance and acquisition
DeviceManagementServiceConfig.Read.All	Read enrollment, Autopilot, filters and service configuration	Core and acquisition
Policy.Read.All	Read Conditional Access and named-location dependencies	Full suite and acquisition when CA is included
Group.Read.All	Resolve assignment group IDs to names and approved membership analysis	Full suite and optional analysis
Directory.Read.All	Read directory objects required for correlation and application evidence	Full enterprise suite
Device.Read.All	Correlate Entra and Intune devices	Duplicate-device assessment and acquisition
DeviceManagementRBAC.Read.All	Read Intune RBAC definitions, assignments, scopes and scope tags	Governance
DeviceManagementScripts.Read.All	Read remediation and script evidence	Operations

Explicitly prohibited assessment permissions and actions

- Directory.ReadWrite.All and all Intune ReadWrite delegated/application scopes.
- Policy.ReadWrite.ConditionalAccess and any Conditional Access modification.
- PATCH, PUT, or DELETE Graph operations in assessment runtime.
- Device retire, wipe, delete, sync, remediation execution, application assignment, policy creation, or configuration change.
- Use of credentials, tokens, or secrets outside the approved session and storage process.

Report-query clarification: Microsoft Intune report exports may require POST requests to /deviceManagement/reports/. These requests query report data and do not alter tenant configuration.

Client authorization statements

- The client authorizes Endpoint Assurance Group and John Jankowski to perform the selected read-only assessment during the approved window.
- The client confirms the tenant GUID and approved operator identity are correct.
- The client understands that evidence limitations and manual validations may remain when Microsoft APIs, licensing, or tenant state prevent automated observation.
- The client understands that framework mapping is alignment evidence and not certification or an audit opinion.
- Remediation, migration, pilot, and production changes require separate written approval and change control.

Revocation and closeout

The client may revoke consent or disable the delegated account at any time. At closeout, the operator will disconnect the Graph session, the client may revoke consent, and evidence will be retained, transferred, or destroyed according to written instructions.

Authorization and acceptance

The parties acknowledge the scope, assumptions, client responsibilities, access model, fees, and delivery conditions stated in this document. Electronic signatures and counterparts are acceptable where permitted by the parties.

Client	Endpoint Assurance Group
Name: _____	John Jankowski
Title: _____	Principal Consultant
Signature: _____	Signature: _____
Date: _____	Date: _____