eido

Data Collected By Eido

Eido Data Collection Statement: Microsoft Graph & Entra ID

EIDO FOR ENTERPRISE

Technical Overview

This document describes the data Eido collects from Microsoft Graph and Entra ID (Azure AD). User and identity data is listed field by field. Device data is summarised by category, as it consists of standard Microsoft Intune management telemetry.

1. User & Identity Data (Entra ID)

1.1 User accounts

Eido collects the following fields from each user account. No other user fields are collected.

Field	Description
Object ID	Unique identifier for the user.
User principal name	Sign-in name (e.g. jane@contoso.com).
Display name	The user's display name.
Email address	Primary email address.
User type	Member or Guest.
Account enabled	Whether the account can sign in.
Office location	Office location.
City	City.
State	State or province.
Country	Country.
Company name	Company name.
Department	Department.
Employee type	For example, Employee or Contractor.
Usage location	Licensing region code.
Preferred data location	Preferred data location.

Field	Description
On-premises security identifier	On-premises AD identifier (for hybrid-joined accounts).
On-premises extension attributes	The 15 custom extension attributes (see 1.2).

Eido does not collect: passwords or any credential material, multi-factor or authentication methods, sign-in history, mailbox or file content, manager or reporting relationships, job title, phone numbers, photos, license assignments, or any field not listed above.

1.2 Extension attributes

Eido collects the 15 standard Entra extension attributes (extensionAttribute1 to extensionAttribute15). These are custom fields defined by your organisation; their contents vary. Empty attributes are not collected.

1.3 Group information

Eido collects the following details about your groups:

Field	Description
Object ID	Unique identifier for the group.
Display name	Group name.
Description	Group description.
Email address	Group email address.
Mail nickname	Group email alias.
Mail enabled	Whether the group is mail-enabled.
Security enabled	Whether the group is a security group.
Security identifier	Group security identifier.
Created by	Application that created the group.

Field	Description
Created date	When the group was created.
Deleted date	When the group was deleted, if applicable.

This is information about the groups themselves. It does not include group membership, except as described below.

1.4 Group membership

Eido collects group membership only for groups your organisation explicitly selects. If no groups are selected, no membership data is collected. For each selected group, Eido collects the member's object ID, display name, user principal name (for users), device ID (for devices), and whether the account is enabled.

1.5 Device extension attributes

For registered device objects, Eido collects only the device ID and the device's extension attributes. (Full device inventory is described in the next section.)

---

2. Device Data (Microsoft Intune)

Device data is standard Microsoft Intune management information. The categories below summarise what is collected.

Category	What it contains
Device inventory	Device name, operating system and version, ownership, enrollment and management state, primary user, last check-in, serial number, model, and manufacturer.
Hardware inventory	Processor, memory, storage, BIOS/firmware version, TPM, network identifiers, and similar hardware details.
Compliance	Device compliance state and per-policy compliance status.
Configuration policies	Configuration profile status per device, plus policy definitions and assignments.
Managed apps	Install status of assigned applications per device.

Category	What it contains
Discovered apps	Inventory of installed applications detected on devices.
Policies & settings	Compliance, configuration, and app-protection policy definitions, assignments, and settings.
Autopilot	Autopilot deployment status.
Certificates	Enrollment certificates and, where applicable, device certificate inventory.
Security & health	Remediation results, firewall status, health attestation, TPM attestation, Defender agent status, active malware, remote-assistance sessions, and elevation events.
App licensing (Apple VPP)	Volume Purchase Program app license data.
App metadata	App icons, descriptions, and catalogue details.
Audit logs	Intune administrative audit events (record of changes made in Intune).
Warranty & product specifications	Warranty and factory specification data, retrieved from device manufacturers (Lenovo, HP) by serial number.

3. Summary

- Eido collects a fixed, explicit list of identity fields, plus standard Intune device telemetry.
- Eido does not collect passwords or credentials, authentication methods, user sign-in history, or mailbox and file content.