

Google Drive voorwaardes vir beperkte-scope datatoegang

Hierdie voorwaardes verduidelik watter Google Drive-toegang DynamicMail versoek wanneer 'n gemagtigde tenantgebruiker of administrateur Google Drive vir tenantdokumentwerkstrome koppel.

Google Sign-In identiteits-scopes soos openid, email en profile is apart van hierdie Google Drive datatoegang-toestemming. Om met Google aan te meld beteken nie dat Google Drive-toegang aanvaar is nie.

Scope

DynamicMail versoek <https://www.googleapis.com/auth/drive> slegs wanneer 'n gemagtigde tenantgebruiker of administrateur Google Drive vir tenantdokumentwerkstrome koppel. Dit is 'n breë restricted Drive-scope wat DynamicMail kan toelaat om alle lêers in die gekoppelde Google Drive-rekening te bekyk en te bestuur, insluitend lêers wat die gebruiker besit, lêers wat met die gebruiker gedeel is, vouers en shared-drive-inhoud wat vir daardie rekening beskikbaar is.

DynamicMail moet die Drive-scope slegs gebruik vir bekendgemaakte, sigbare Drive-dokumentwerkstrome wat deur die tenant gekies is.

Data waartoe DynamicMail toegang kan hê

Wanneer Google Drive gekoppel is, kan DynamicMail toegang hê tot Drive-data wat nodig is om die gekose tenantwerkstroom te lewer, insluitend:

- lêer-ID's, name, MIME-tipes, kontrolesomme, grootte, tydtempels, beskrywings, etikette, vouerverwysings, ouervouers en ander lêermetadata;
- vouermetadata, shared-drive-metadata en soek- of lysresultate wat nodig is om tenantdokumente te vind;
- lêerinhoud, voorskoue, kleinkiekies, uitvoere, aflaaie, oplaaië en gegenereerde of geredigeerde lêerpayloads;
- deel- en toestemmingsmetadata wanneer dit nodig is om 'n sigbare Drive-lêerhandeling te wys of te voltooi;
- rekeningvlak Drive-opsommingsinligting wat nodig is om die gekoppelde rekening en verbindingstatus te bevestig;
- gestoorde kopieë of gekaste uittreksels van Drive-lêers wat in DynamicMail ingevoer is;

- afgeleide data wat uit Drive-lêers geskep word, soos OCR-teks, geparseerde dokumentvelde, klassifikasie-etikette, uittrekresultate, opsommings, ouditgebeurtenisse en dokumentrekords.

DynamicMail mag nie Drive-data versoek, deursoek, kopieer, aflaai, wysig, verwyder of andersins verwerk wat nie met die sigbare Drive-dokumentwerkstroom verband hou nie.

Doel

DynamicMail gebruik Google Drive-data om Drive-dokumentwerkstrome te lewer wat tenants gekies het. Die beoogde doeleindes is:

- om gemagtigde gebruikers Drive as 'n dokumentbron of dokumentbestemming te laat koppel;
- om tenantbesigheidsdokumente te vind, te lys, in te voer, af te laai, uit te voer, op te laai of by te werk wanneer dit deur die produkvloei gekies is;
- om Drive-dokumente te onttrek, te klassifiseer en na DynamicMail-werkstrome te roeteer;
- om verbindings-, lêerhandeling-, sinkronisasie- en verwerkingstatus aan gemagtigde tenantgebruikers te wys;
- om ouditrekords en bedryfslogboeke te hou wat bewys watter Drive-handeling versoek en voltooi is;
- om foutopsporing, sekuriteit, misbruikvoorkoming, geskilhantering en regsnakomingsaktiwiteite uit te voer wat deur die toepaslike beleide en die tenantooreenkoms toegelaat word.

DynamicMail mag nie Google Drive-data verkoop, dit vir advertensies of retargeting gebruik, dit aan datamakelaars oordra, dit vir toesig gebruik, of dit gebruik om kredietwaardigheid of geskiktheid vir lenings te bepaal nie.

Breë Drive-scope en nouste scope

Die <https://www.googleapis.com/auth/drive> scope is breed omdat dit toegang kan toelaat tot alle Drive-lêers wat vir die gekoppelde rekening beskikbaar is. DynamicMail moet hierdie scope as voorlopig behandel totdat produk- en nakomingsbeoordeling dokumenteer waarom nouer Drive-scopes onvoldoende is vir die geïmplementeerde werkstroom.

Voor produksiegebruik behoort DynamicMail nouer Drive-scopes te evalueer, soos `drive.file`, `drive.readonly`, `drive.metadata.readonly`, `drive.appdata` of `drive.appfolder`. As 'n nouer scope die sigbare funksie kan ondersteun, moet die versoekte scope, toestemmingsrekords, OAuth-konfigurasie, bronasset, gerenderde asset en toetse voor vrystelling bygewerk word.

Bewaring

DynamicMail bewaar Drive-afgeleide data slegs so lank as wat dit nodig is vir die sigbare Drive-werkstroom, tenantinstellings vir dokumentbewaring, ouditrekords, sekuriteit, geskilhantering of regsnakoming. OAuth-tokens en Drive-handelingmetadata word slegs bewaar so lank as wat dit nodig is om die gekoppelde Drive-integrasie te laat werk of vereiste ouditrekords te behou.

Drive-lêerinhoud, gekaste lêers, metadata, OCR-teks, onttrekte velde en afgeleide dokumentdata behoort verwyder of geanonimiseer te word wanneer dit nie meer nodig is vir die bekendgemaakte doel nie, tensy 'n regs-, sekuriteits-, oudit- of tenantbewaringsverpligting verdere bewaring vereis.

Verwydering

'n Gemagtigde tenantgebruiker of administrateur kan verwydering versoek van Google-afgeleide gekaste data, ingevoerde Drive-lêers, onttrekte teks en afgeleide dokumentrekords. DynamicMail behoort die versoekte data te verwyder of te anonimiseer wanneer die tenant se bewaringsinstellings en toepaslike wetgewing dit toelaat.

Die verwydering van ingevoerde DynamicMail-rekords verwyder nie noodwendig die oorspronklike lêer uit Google Drive nie. DynamicMail mag oorspronklike Drive-lêers slegs wysig, skuif, na die asblik skuif of verwyder wanneer 'n gemagtigde gebruiker daardie Drive-handeling uitdruklik deur 'n sigbare produkwerkstroom versoek en die handeling deur tenantbeleid en toepaslike wetgewing toegelaat word.

Intrekking en ontkoppeling

Die tenant kan Google Drive in DynamicMail ontkoppel. Na ontkoppeling of plaaslike intrekking van toestemming moet DynamicMail ophou om gestoorde OAuth-tokens vir Google Drive te gebruik en moet DynamicMail ophou om bykomende Drive-lêers uit die gekoppelde rekening te lees, te skryf, af te laai, op te laai, te wysig of te verwyder.

Die Google-rekeningeienaar kan ook die app-magtiging in Google-rekeninginstellings intrek. As Google-magtiging ingetrek word, moet DynamicMail Drive API-toegang stop wanneer tokenvernuwing of API-oproepe misluk, en die verbinding behoort as ontkoppel of as herverbinding vereis gewys te word.

Plaaslike intrekking verwyder nie outomaties reeds ingevoerde DynamicMail-dokumente nie. Daardie rekords word volgens die verwyderings- en bewaringsreëls hierbo hanteer.

AI, OCR en uittrekking

DynamicMail kan OCR, parsing, klassifikasie, opsomming en ander AI-ondersteunde verwerking op Drive-lêerinhoud en metadata toepas, slegs om die sigbare tenant Drive-dokumentwerkstroom te lewer of te verbeter. Drive-data en afgeleide data mag nie

gebruik word om 'n algemene masjienleer- of AI-model buite die tenant se versoekte funksie te skep, op te lei of te verbeter nie.

AI-ondersteunde resultate kan verkeerd wees. DynamicMail behoort onttrekte data as werkstroomuitvoer aan te bied wat gemagtigde gebruikers volgens die produkvloei kan nagaan, regstel, goedkeur, verwerp of verwyder.

Ondersteuning en menslike toegang

DynamicMail-personeel, kontrakteurs of subverwerkers behoort nie spesifieke Drive-lêers, onttrekte teks, lêermetadata of afgeleide Drive-data te lees nie, tensy een van hierdie voorwaardes geld:

- die gebruiker het uitdruklik ondersteuning versoek wat toegang tot spesifieke data vereis;
- toegang is nodig vir sekuriteitsondersoek, misbruikvoorkoming of insidentreaksie;
- toegang is nodig om aan wetgewing, regsproses of 'n bindende tenantinstruksie te voldoen;
- die data is vir interne bedrywighede geaggregeer of geanonimiseer en geen spesifieke gebruiker se Drive-inhoud is leesbaar nie.

Ondersteuningstoegang behoort minste-voorreg te wees, waar prakties tydsbeperk te wees, en vir ouditbaarheid gelog te word.

Dit is gelokaliseerde implementerings- en beoordelingsmateriaal, nie finale regsadvies nie. Dit mag nie sonder afsonderlike beoordelingsbewys aangebied word as bewys van Google-goedkeuring, eksterne regsgoedkeuring of produksieklaring vir beperkte scopes nie.

Verwysings

- DynamicMail restricted-scope contract:
Documentation/DynamicMail/LocalizedIntegrations/google-restricted-scope-compliance-contract-2026-06-02.md
- Google API Services User Data Policy: <https://developers.google.com/terms/api-services-user-data-policy>
- Google Workspace API user data and developer policy:
<https://developers.google.com/workspace/workspace-api-user-data-developer-policy>
- Google Drive API scopes:
<https://developers.google.com/workspace/drive/api/guides/api-specific-auth>
- Google restricted-scope verification guidance:
<https://developers.google.com/identity/protocols/oauth2/production-readiness/restricted-scope-verification>