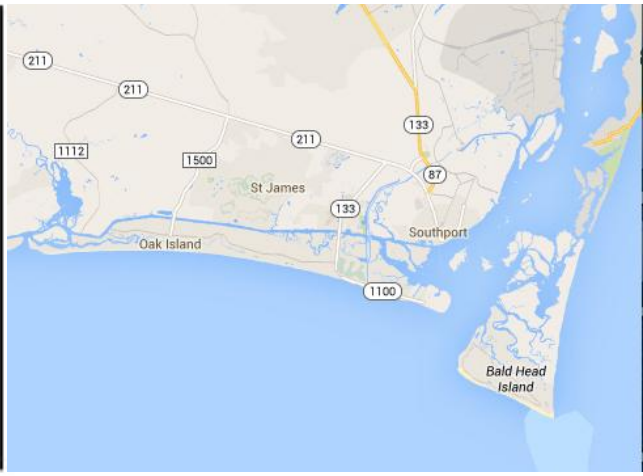
Google Maps for Work

Google Maps Engine Approach to IT Security



Introduction

Google Maps Engine

Google Maps Engine (GME) is a cloud-based geospatial platform that lets organizations layer their data on top of Google's base map and create custom maps and applications. It incorporates Google Maps' familiar technology and user interface, making it easy to publish beautiful maps and share them with stakeholders. Built on the same platform that provides Google services to millions of people worldwide, users have a consistent and reliable maps experience wherever they are.

This paper is a companion paper to Google's Common Security White Paper (GCSWP), and is focused on the security related topics specific only to Google Maps Engine. This paper will describe the ways in which Google ensures security across the entire workflow process and interactions inherent to Google Maps Engine. This includes topics such as data ingest, processing, sharing, authentication, APIs, privacy, location, logging and data deletion.

The policies described in this paper are detailed as of the time of authorship. Google will make every attempt to update this document as we update the product with new features and functionality.

Projects

Google Maps Engine

A GME project is a unique account generated for a customer that provides them with dedicated storage and serving quota for uploading data and creating and publishing maps. At the time of provisioning, each GME project is assigned a project ID that is 20 digits long (e.g. 11613121305523030954). This unique ID is encoded in many of the GME serving URLs generated for maps and data, and is how GME knows to associate quota use with a given project. The ID is an obfuscated version of a generated internal ID, and does not contain any sensitive information and there is no way to use it to gain access to protected information.

User Roles

Google Maps Engine

GME users fall into one of the three roles described below. Membership in these user roles permit various levels of access to hosted maps and data.

Map Viewers
Map Viewers are the external users who are granted access to view, query and interact with published GME assets (maps, layers and data). In the case of GME assets that are open to the public, Map Viewers refers to anyone who accesses a GME asset.

Map Editors
Map Editors are the day to day map authors and data custodians who are granted access to the GME project by Project Administrators. In addition to everything Map Viewers can do, Map Editors can create, upload, style, modify and delete data and create and publish maps using this data. Map Editors also can view project quotas and usage statistics for the maps and data they have access to, and can see the list of users (names and email addresses) and/or groups (member list is obscured) who can access any of the GME assets a they themselves have access to.

Project Administrators
Project administrators have the broadest set of permissions and are considered super-users for
a GME project. In addition to everything Map Editors and Map Viewers can do, Project Administrators can:

- Access and manage all data hosted within a single GME project
- Add or remove other Project Administrators
- Change the publishing permissions for Map Editors

Authentication

Google Maps Engine

GME relies on Google's standard user-based authentication service to securely authenticate and identify all users. This is the same system used by products such as Google Apps and explained in more detail in the GCSWP.

There are two categories of authentication:

- Google Account authentication to validate a user's identity
- Maps Engine authorization for access to GME assets

Google Account Authentication
Users signing in with their Google Accounts are authenticated using the standard Google Accounts service that is more fully described in the GCSWP.

Google allows for the use of a two-factor (2-step) authentication process. This adds a second layer of security to the login process for Project Administrators, Map Editors and Map Viewers. The default 2-step verification system requires users to enter a 6-digit, one-time password (OTP), which is generated by a mobile app or hardware token, in addition to a password, when signing into GME. Information about 2-factor authentication can be found at the Google Apps security site.

Google and Google Maps Engine (GME) also offer a Security Assertion Markup Language (SAML) based Single Sign-On (SSO) option to delegate the authentication authorization event to a third-party. This allows a GME customer to integrate their own identity provider into the SAML transaction process. In this arrangement, Google acts as the service provider

When the now-authenticated user requests access to GME content, the request is authorized differently based on the nature of the request. Details follow:

Content Authorization through the Maps Engine UI (User Interface)
GME maintains a mapping between each Google user and the GME projects (and roles within those projects) they have access to. When a user navigates to mapsengine.google.com, GME relies on the existence of the aforementioned cookie to verify their identity. GME then dereferences the projects they can access and presents them to the user in the GME project drop-down.

GME sets a cookie to remember the last project the user was using, to bring them back to it when they return.

Content Authorization for Maps Engine Tile and KML Serving (Desktop, Mobile, Web)
When a user then makes a request to GME for an access-controlled map, map tile or to stream KML from an application or within custom code, the following occurs:

1. The calling application or client passes the users aforementioned cookie along with the request, which permits the GME servers to identify the the user who made the request.
2. Initial requests to GME are sent to an authentication server for validation prior to subsequently being sent to the various GME backends to fetch data or access objects.
3. When the GME service receives the request, it first verifies whether or not the authenticated user has access to the object in question according to the GME managed mapping between users and GME objects. If the user does have access and can perform the desired action, the GME server generates a short lived bearer token to grant access to the object on behalf of the user. This token is sent back to the requesting client which in turn appends it to subsequent requests to the appropriate backend to fetch that object.

The short lived bearer token generated by GME to grant access to the various GME servers and backends has no personally identifiable information stored in it. The token was designed to expire after a short period (currently 60 minutes), and to be fast to decrypt such that it can be sent with every single request for a tile or other GME data object.

Requests to public data bypass the above process and access the GME asset directly.

Sharing

Google Maps Engine

GME relies on the same sharing infrastructure used by other Google products such as Google Docs and Spreadsheets. Like Docs and Spreadsheets, each object in GME has an access control list (ACL) associated with it that defines the users who can access it and the type of access they have. Unlike Docs and Spreadsheets, GME differentiates between sharing controls on the draft version of an object and sharing controls on the published version of that object.

Map Editors with edit privileges on an object can modify its draft and published version ACLs.

Draft Version Sharing
The draft version of an object is the version of it that can be accessed by Map Editors, typically for the purposes of making changes to it and when ready, promoting those changes to the published version for viewing by Map Viewers. Users can be added to the draft version ACL with read only or read/write privileges. All modifications to an object happen to the draft version.

Published Version Sharing
The published version of an object is the version of it that can be accessed by Map Viewers. Users can be added to the published version ACL with read only privileges. It is not possible to edit the published version of an object.

Data

Google Maps Engine

Data uploaded to GME goes through a security sanitization process and subsequently a normalization process in order to turn it into the formats GME uses to make it mappable. Details about these processes follow.

Upload
Users can upload their GIS data to GME through the web interface, APIs or certain third party products. All uploads are secure and happen over encrypted HTTP (HTTPS).

Under certain circumstances Google may work with the customer to electronically fetch their data, and/or the customer may also choose to send data to Google using a physical media type, like a hard drive or a DVD. It is beyond the scope of this document to describe the policies and procedures Google adheres to when managing data shipped physically to Google for manual upload.

Once uploaded to GME, a copy of the customer data goes through a security sandboxing process that translates the data into a neutralized format from which it can subsequently be processed into maps. This neutralization process strips potentially malicious information from the data and ensures the integrity of the data prior to further use.

Once the neutralized format is created, the GME systems then ingest the data into the relevant backend datastore. There are separate datastores for each of the primary types of data -- imagery, terrain and vector.

Deletion
Data created and stored within GME, including uploaded data and all derived data products from it remains active on Google Servers while the GME project is valid and the objects themselves are not explicitly deleted. Map Editors can delete any dataset through the GME web interface, and in doing so the data will be (1) immediately hidden from the GME interface and API; (2) purged from the main GME application servers within 30 days; and (3) purged from all backup servers within an additional 30 days.

Privacy
GME data is held separately from the Google-owned or licensed data that is part of Google Maps or Earth products. Except for under a separate written agreement, Google has no rights to use customer uploaded GME data for its public Maps and Earth products.

Google engineers may from time to time require access to customer GME data, but only for the purposes of debugging customer support tickets.

Project Termination
If a customer chooses not to continue their use of GME by not renewing their project, then at the end of the term the GME project will be switched to a disabled state preventing Project Admins and Map Editors from accessing it through the UI, and Map Viewers from accessing any published maps or GME assets. The customer then has 30 days to renew before GME irrevocably commences deletion of all customer data. Customer data is guaranteed to be deleted from Google servers by 180 days after this process has commenced.

Location
Customer data and all derived data products from it may be replicated across Google's worldwide multi-tenant architecture. This infrastructure provides access to distributed machines across multiple data centers, and enables faster processing and low latency serving to customers anywhere on the planet.

Logging

Google Maps Engine

GME follows Google's general logging principles and policy, as defined in GCSWP. Across the GME services, logs are maintained for between 7 and 63 days on Google's servers. These logs may contain personally identifiable information such as the identity of an end user requesting access to view a map, the name of the project that owns the data or map, or the identity of a user uploading data to GME. Logs are accessible by a limited set of Google software and support engineers. After the retention period these logs are deleted from Google servers.