LOGZILLA DOCUMENTATION

GeoIP

Rules to add geolocation for Src and Dst IPs

LogZilla App Store · Generated June 12, 2026 · logzilla.ai/docs/logzilla-appstore/geoip

Overview

The GeoIP app adds geographic location information to events based on IP addresses. It uses MaxMind GeoIP databases to look up city, state, and country information for source and destination IP addresses.

App Function

The GeoIP app is a *supplemental* app. It is not stand-alone; it is intended to run after other user-specified apps run. Prior apps will set the `SrcIP` and `DstIP` user tags based on their own functioning. Then the GeoIP app will use geoip lookup for both `SrcIP` and `DstIP` and set additional tags with that information.

Vendor Documentation

- MaxMind GeoIP Databases (https://www.maxmind.com/en/geoip2-databases)

Device Configuration

No device configuration is required. The GeoIP app automatically processes events that have `SrcIP` or `DstIP` user tags set by other apps.

Incoming Log Format

The GeoIP app does not process logs directly. It processes `SrcIP` and `DstIP` user tags that are set by other installed apps.

Parsed Metadata Fields

Tag Name	Example	Description
`SrcIP City`	`Atlanta`	City for source IP
`SrcIP State`	`Georgia`	State or province for source IP
`SrcIP Country`	`United States`	Country for source IP
`DstIP City`	`Toronto`	City for destination IP

Tag Name	Example	Description
`DstIP State`	`Ontario`	State or province for destination IP
`DstIP Country`	`Canada`	Country for destination IP

Note that in some cases the geoip lookup is not able to determine specific location information, in which case usually the country is available but the city and state may not be. The city, state, and if applicable country fields will be set to `Unknown` for these cases.

Log Examples

The GeoIP app does not process logs directly. It enriches events that already have `SrcIP` or `DstIP` user tags set by other apps.